TAMPEREEN TEKNILLINEN YLIOPISTO
TAMPERE UNIVERSITY OF TECHNOLOGY

MUHAMMAD ATHER FAYYAZ

NETWORKING CAPABILITIES OF IEEE 802.11S AND IEEE 802.11AH SYSTEMS

Master of Science Thesis

Examiner: Prof. Mikko Valkama
Examiner and topic approved by the
Faculty Council of the Faculty of
Computing and Electrical Engineering
on 26 Oct 2015

ABSTRACT

MUHAMMAD ATHER FAYYAZ: Networking capabilities of IEEE 802.11s and IEEE 802.11ah systems
Tampere University of Technology
Master of Science Thesis, 67 pages
August 2016
Master's Degree Programme in Information Technology
Major: Communication Systems and Networks
Examiner: Prof. Mikko Valkama
Keywords: sensors, IoT, internet of things, mesh networks, relays, efficiency, throughput, Ieee 802.11ah, Ieee 802.11s

Internet of Things was considered a new technology couple of years ago but with the speed at which technologies are improving and being implemented, we can see IoT devices and platforms already in market. But sadly, there is still no concensus on how these devices would unanimously commmunicate with each other. Thankfully IEEE 802.11ah brings up a unanimous and unique way for all these devices to communicate and coexist on lower 2 layers of OSI model. 802.11ah can communicate with other networking protocols as well and interestingly, dedicated Application layer protocols for IoT (COAP) are also being implemented these days. IEEE 802.11ah is simulated in this thesis and also the relaying option from the draft is implemented.
IEEE 802.11s mesh on the other hand is rather old technology but still serves the purpose really well and is implemented in various situations. Because of nice and detailed networking infrastructure of IEEE 802.11s mesh, this protocol is studied and simulated in this thesis. However, to make the scenario closer to IoT use case, only stationary devices are used and hence Proactive networking protocols of Mesh are deemed better suited. We analyse the networking bits of both these technologies in this thesis to see if they can coexist and cooperate.
In the end, we mention the performance of these technologies and propose some future enhancements.

PREFACE

The research work for this Master of Science Thesis was conducted during the academic year 2015 - 2016 with Department of Electronics and Communications Engineering, Tampere University of Tecnhology .
I would like to thank my supervisor Prof. Mikko Valkama for investing his time and knowledge in this study. I would also like to thank Dr. Ali Hazmi for getting me started with this thesis on the right foot and for his appreciation and support. I would like to extend my thanks to Msc Quttab-ud-din Qazi for his support and help while understanding the coding part for this thesis. I would also like to thank MSc Orod Raeesi for sharing his knowledge and understanding of wireless sensor networks and specially 802.11ah technology.
Finally I would like to express my deepest gratefulness to my family, especially my parents who are the motivation behind my success, who supported me all this time in all ups and downs of my life, who loved me unconditionally and believed in me no matter what. I feel like I owe every part of my life to my parents for they are the compelling force behind me.

August, 2016
Muhammad Ather Fayyaz

TABLE OF CONTENTS

LIST OF FIGURES

LIST OF ABBREVIATIONS AND SYMBOLS

TUT	Tampere University of Technology
IEEE SA	Institute of Electrical and Electronics Engineers Standardization Authority
Sub 1 GHz	Less than 1 GHz frequency.
OSI	Open Systems Interconnect
AP	Access Point
STA	Station / Sensor in this context.
MIMO	Multiple Input Multiple Output
SISO	Single Input Single Output
peer to peer	peers are computer systems which can communicate with each other and don't necessarily need a central device.
client - server basedclient	computers initiate a request to server computers for data transfer.
unicast	one to one tyoe of communication between computers or communication systems
multicast	one to many type of communicaiton between computers or communication systems.
broadcast	one to all type of communicaiton between computers or communications systems
WiFi	Wireless Fidelity, mostly IEEE 802.11 suite of protocols for lower 2 layers.

OSI	Open Systems Interconnect

1. INTRODUCTION

There has been huge advancement in technology in last couple of years and specially in communication technology. Scientists, researchers and engineers have developed 5G communications, vehicle to vehicle communications, smart networks, optical fiber communication, big data, Internet of things and many more interesting communication infrastructures. These advancements in technology along with Electronics and Battery size reduction resulted in various kinds and sizes of devices for personnal as well as public use (for example sensor networks for public safety, sensing environment and much more). One part that all these devices have in common is communication. All these devices need to communicate to one another in some fashion. Some are peer to peer based while others are client - server based. In other words, some devices unicast, some multicast while other devices broadcast. This communicating devices have lead to different kinds of communication networks, some peculiar to some specific scenarios while others more general.

Institute of Electrical and Electronics Engineers (IEEE) is an organization constituting of Engineers, Scientists, Researchers and allied professionals. It is created to serve professionals belonging to all fields of Eletrical, Electronics and Computing industry and it strives to provide innovative and in-depth technologies related to the mentioned fields.[1] One broad, well known, accepted and practised communication suite of protocols all around the world is WiFi. Wireless Fidelity (WiFi), also called Wireless Local Area Network (WLAN), is an IEEE suite of protocols which defines MAC and Phy layers of OSI reference model in order to connect devices to any other network. [2] [3] Open Systems Interconnect model describes how data is transfered from a software on one computer to a software on another computer in terms of seven layers. This reference model was advised in 1984 by International Standardization Organization ISO and is now used as primary reference in all modes of communication platforms. The important part to notive is that data starts from 7th layer and as it goes down layers in the OSI later model, each later adds its own

information in form of header and finally, physical layer transmits data along with header in the form of signals on physical medium. The physical layer of receiving computer receives the signal, extracts information from its own layer's header and passes the datagram upwards and the same process repeats until the data reaches Application layer where it is transfered to the destination software. [4]. Briefly, the seven layers and their functions are described below. The diagram 1.1 also shows how these layers can communicate to another computer in a network with intermediate devices in between.
Application Layer, user interacts with software on this layer.
Presentation Layer, provides coding and presentation of data to be readable by application layer.
Session Layer, established, manages and terminates the communication session.
Transport Layer, is mainly responsible for realiable and unrealiable communicaiton of data, some example functions are flow control, multiplexing, error check and recovery etc.
Network Layer, provides routing over the network by using various routing protocols.
Data Link Layer, provides flow control, error checking and correction and addressing for local area network.
Physical Layer, tranceives signals on physical medium.

Since lowest 2 layers are defined in this IEEE 802.11, the rest of layers in OSI reference model remains the same and all IEEE 802.11 protocols work in same way with those upper layers. The idea for different protocols on MAC and Phy layer, introduced by IEEE 802.11, is to cater different devices working on different frequencies under different circumstances. We will discus 2 of these protocols IEEE 802.11s and IEEE 802.11ah in this thesis. The basics of WiFi/WLAN is defined in chapter 2.
IEEE 802.11s, as detailed in chapter 3, is a wireless mesh networking protocol which gives us the ease of wireless networking not only on access level but also on distribution level. The main implementation areas for wireless mesh network could be public wifi, hospitals or office buildings or even houses where there are many number of devices connecting to the network and don't want the connection to get slow or disconnect everytime device's position is in a corner (geographically), mesh network solves this by relaying data through th nearest available device and also the network is resilient for link breakages. More details about this technology and simulation analysis is in chapter 3. The other IEEE 802.11 protocol that is analysed in this

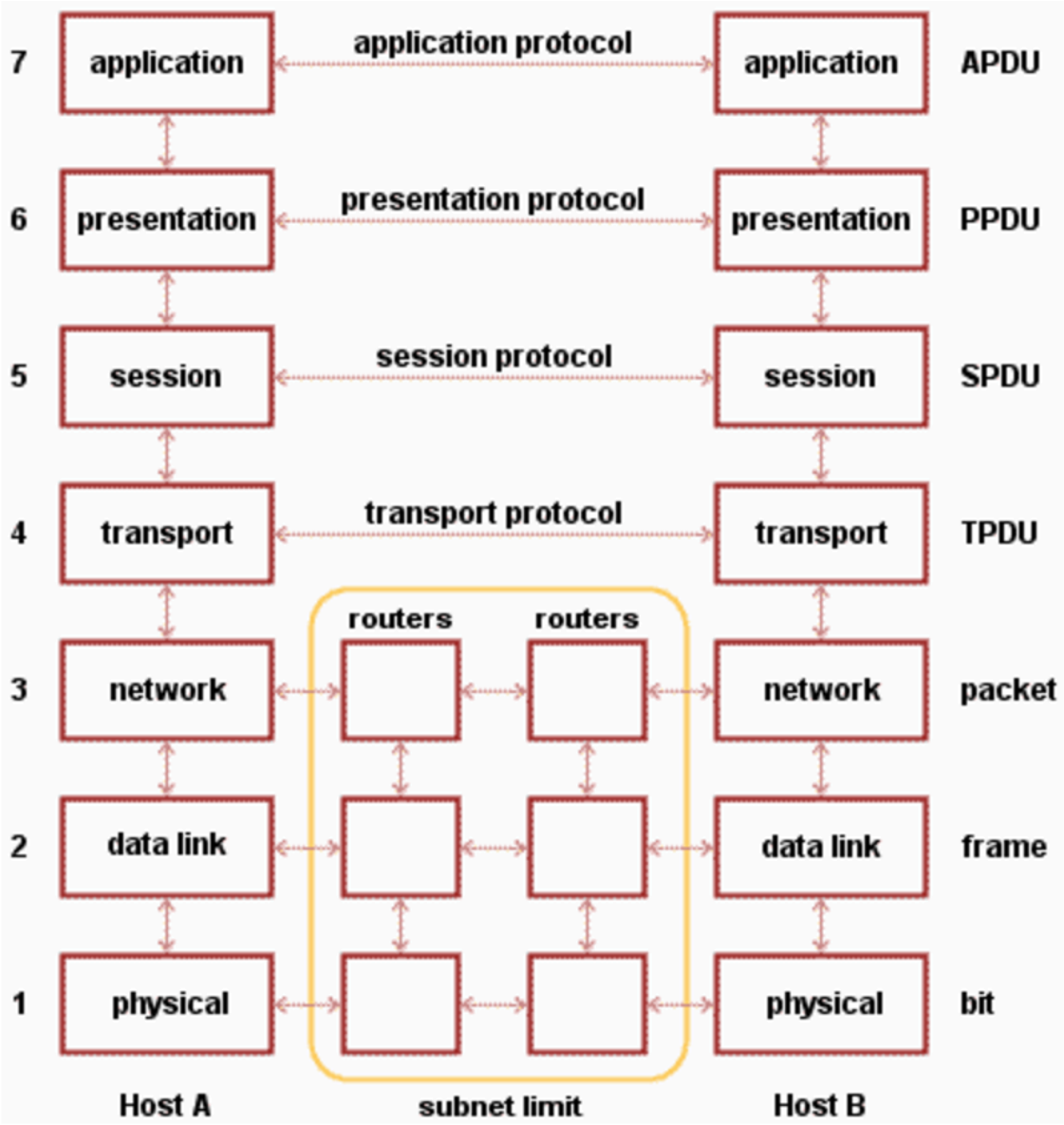


Figure 1.1 *OSI layers communicating with each other over the network*

thesis is IEEE 802.11ah. As there are a lot more number of devices available now than there used to be one decade ago, all these new and advanced devices need to stay active on battery power for long time and also communicate. IEEE had set up a Task Group to come up with energy efficient, long range wireless communication protocol called 802.11ah which will be standardized in late 2016. The main focus of this protocol is Internet of Things, however, this protocol can still be used for various other applications. One of the differentiating things about this protocol is that it uses sub 1 GHz for its operation and not the standard (2.4 GHz/ 5 GHz)

WiFi frequency.
The reason for this analysis and especially these two technologies is to analyse their performance in particular scenarios and since 802.11s is a bit old protocol with quite nice networking insights, the idea of this thesis is to analyse the networking side of both protocols. The new draft release of IEEE 802.11ah already has multi-hop relaying mechanism which introduces some networking but without much use of networking protocols. IEEE 802.11ah is discussed in detail in chapter 4 while chapter 5 entails the summary and combined analysis of both of these technologies. The main limitations of this study was that since IEEE 802.11ah works on sub 1 GHz radio and all the parameters were not completely described at the time of implementatio, we couldn't really get practical hardware working exactly on this specification and so we had to simulate the environment. The environment is quite close to real time environment in simulations. The security aspect of any of these protocols is not considered in this thesis. The merit of judgement of these technologies is throughput and delay mainly. Also IEEE 802.11ah simulations doesn't have real ARP and authentication mechanism to connect to AP, rather the beacon with highest signal strength is considered as viable candidate to connect to, which gives accurate results as with authentication mechanism, once the network is setup.

2. WIRELESS SENSOR BASICS

A wireless sensor network is a wireless network of autonomous devices, distributed in a certain area, monitoring some physical parameter.[5] IEEE introduced 802.11 as a suite of standard protocols for Wireless Local Area Networks. Every computer either portable, mobile or fixed, able to communicate over a network, is reffered to as Station in Local Area Network. Two or more stations communicating with each other form a Basic Service Set. This BSS is a key building block of any network. When this communication takes place wirelessly and the stations are small sensing devices, it forms a wireless sensor network. If this BSS is not connected to any Base station and the participating devices are only communicating with each other, it would be called an Independant BSS (IBSS) or a BSS working in AD-Hoc mode i.e. peers only communicate with other peers in peer to peer fashion. BSSs communicate together through Access Point via a Distribution System DS, in infrastructure based network and this whole hierarchy of BSSs communicating via DS is called an Extended Service Set ESS.[6]

In a BSS when station tries to connect to AP, there are some packets that flow and the communication taking place in between is shown in below diagram: 2.1 This figure explains the procedure of wireless stations connecting to APs. Wireless stations first sends the probe request to look for APs. In this probe request, station sends its supported protocols and data rates. The AP in turn checks if it supports that data rate, then responds with Probe response with its SSID and encryption types. The next step is authentication where station sends authentication request to AP and AP responds with authentication response. The final step is association in which station sends association request with the encryption types that it would like to use and if AP supports that encryption type, AP responds with association response message and after this, the station gets access to the network via AP. Stations can be authenticated to multiple APs at any given but can be associated to any single AP.

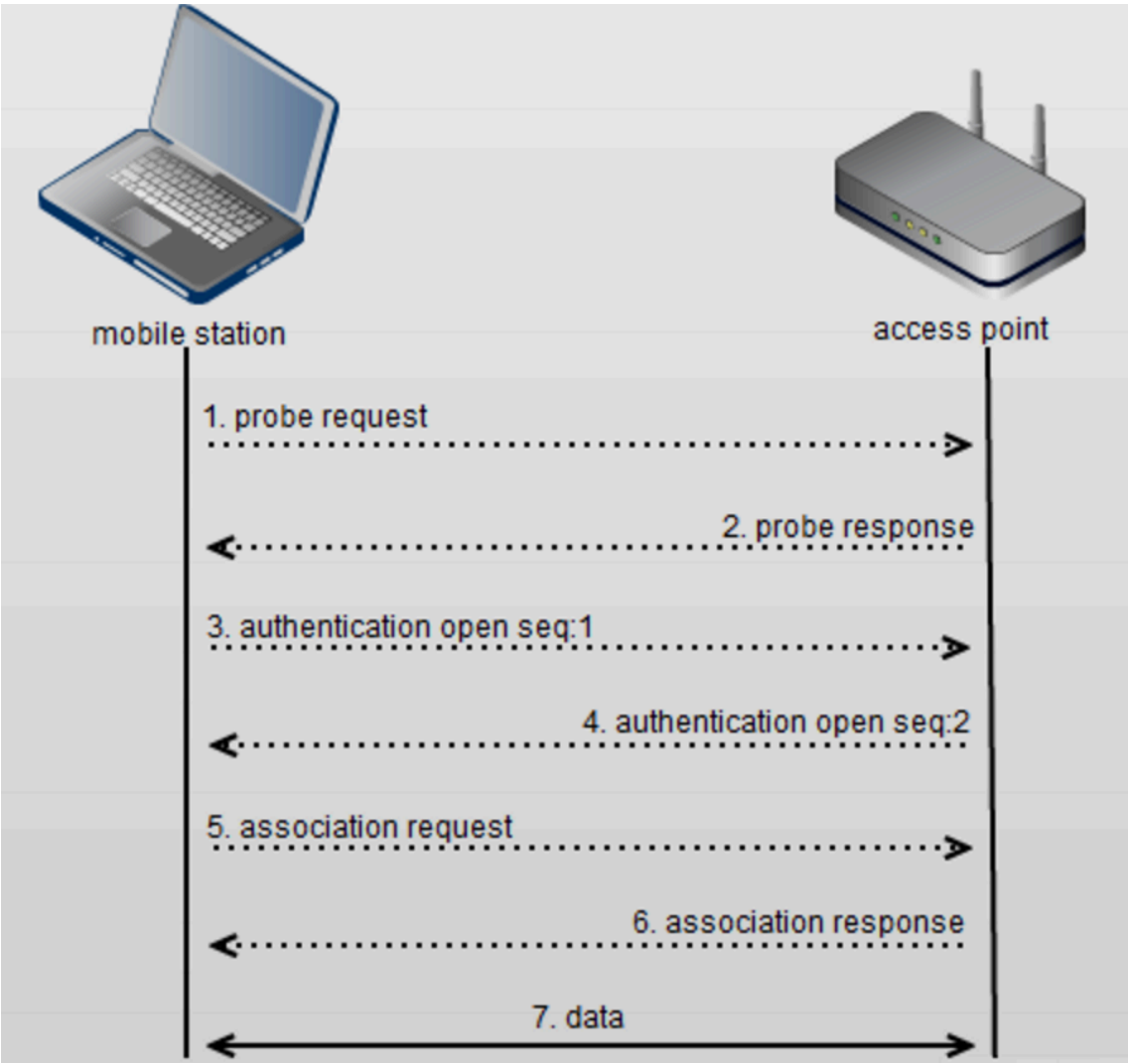


Figure 2.1 *Messages between station and AP*

2.1 Physical Layer

Physical layer deals with tranceiving bits of data in the form of signals on Physical medium. The device used for this purpose is called antenna (in case of wireless). There are different types and configurations of antennas for different purposes but we will not go into that since this thesis is about networking performance of these protocols.

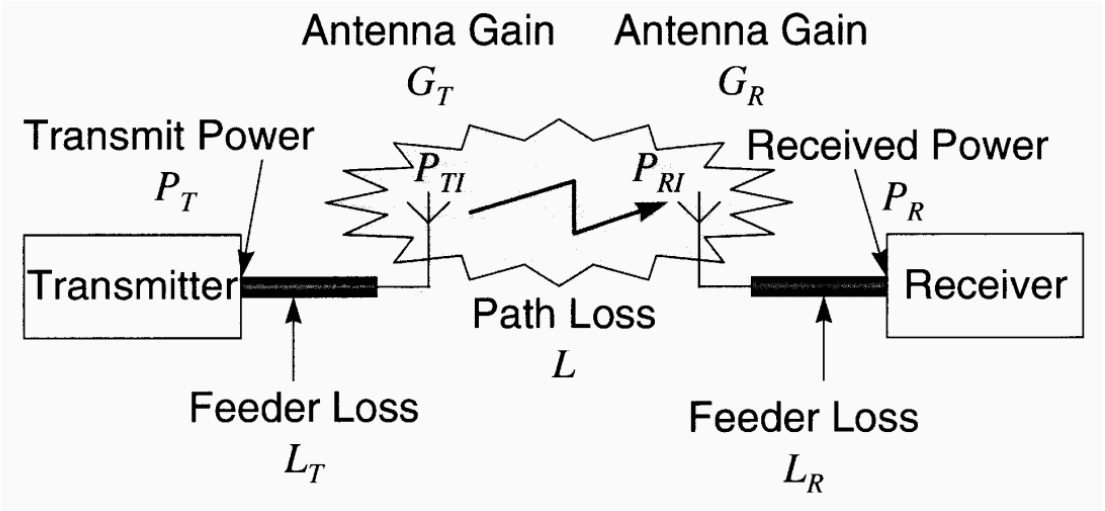


***Figure** 2.2 Link Budget Analysis*

2.1.1 Parameters

If we consider communication from one computing device to another on physical layer, there are couple of paramteres involved, mainly, gain of antenna, noise of antenna (feeder loss), path loss model for whole communication, receiver antenna's gain, noise and sensitivity. Fig 2.2 shows the whole process. Simulations in this thesis consider 0 dB gain in transmitting and receiving antennas and 0 dB feeder loss. Path loss models are models which describe how noise will affect the signal while travelling through medium. It can also be said that path loss is the difference between transmitted power and the received power (in dB) [7] [8].

Path Loss Models

There are many path loss models for outdoors and indoors environmet (empirical, semi deterministic and deterministic), we are considering outdoor Macrocell environment in this thesis for both protocols and their specific path loss models are described in their respective chapters. [7]

Receiver Sensitivity

Receiver sensitivity is a measure of how good or bad a receiver is. The more the sensitivity value, the better is the quality of the receiver (e.g. -110 dBm sensitivity is better than -90 dBm). Sensitivity in itself means minimum signal strength that can be detected as signal, not noise. Therefore, in order to have a successful communicaiton, communication systems are designed in such a way that received power should be more than receiver sensitivity so that this signal could be detected and interpreted as data. [9]. In other words, receiver sensitivity is minimum input signal required to result in a specified output signal with a specific Signal to Noise Ratio SNR. It can be calculated as : 2.1

$$\begin{aligned} Sensitivity(min) &= (S/N) * KTBN \\ K = Boltzmann'sconstant &= 1.38 * exp - 23Joule/K \\ T = absolutetemperature &= 290K \\ B &= Bandwidthofreceiver \\ N &= Noisefigureofreceiver. \end{aligned} \tag{2.1}$$

2.1.2 Multiplexing

Another function that Physical layer provides is multiplexing which is used to send multiple users' data on a single link but here in this case, we are considering networks in which each station is connected to AP so every station has its own link to AP. Also Data Link layer (2nd layer in OSI model) provides segmentation and fragmentation i.e. if data size is larger than maximum transmission unit (mtu) size allowed on a layer, it is divided into small parts called segments and then transmitted. In IEEE 802.11 networks, the default MTU size is 2312 Bytes while Ethernet and ISDN (Integrated Services Digital Network, e.g. land line phones) have 1500 Bytes [10] and overall, its better to have the least mtu size of packtes that any link can support so we will have 1500 Bytes MTU size in all out simulations.

2.1.3 Modulation and Coding Schemes

Modulation and Coding schemes are physical layer parameters to see the data rate used for the ongoing communication. Low frequency data is sent wirelessly by encoding this data on to a high frequency signal so that antenna sizes could be reduced

as antenna size is inversely proportional to frequency. Therefore, transmitting low frequency encoded and modulated signal to a high frequency gives us small antenna sizes to be integrated in devices. Different protocols use different modulation and coding schemes. [11]

2.2 Link Layer

2.2.1 Carrier Sensing and Channel Access

Channel Access

Channel Access schemes depend on which medium is being used e.g. multiple access schemes are used when the wireless channel is shared between many users. These schemes are divided into three types i.e. controlled access / taking turns / polling, channelized access and random access. In controlled access / taking turns, the resources are assigned and managed by Master node. One example of such protocols is Polling in which Master node (usually AP) checks whether Slave nodes (usually stations) have data ready to be sent, if yes, then that Slave node gets the channel otherwise Master keeps checking other slaves. This is also called Dynamic Access. Token Passing is another example which works in a way that token is passed in a round robin fashion among nodes and whichever node has token at any given time, has the opportunity to send its data over the channel. [12]

In channelized protocols, channel is divided among users for specific time, frequency or code and the examples are TDMA, FDMA and CDMA respectively. TDMA systems specify channel access on the basis of Time slots for its users, FDMA systems specify channel access based on different frequencies for different users, and CDMA systems do so by assigning different codes to different users. All these are examples that channel would be accessed by one user for any given resource at any given time. This mode of channel access is called contention free channel access. [13]

Random access protocols involve stations randomly accessing channel on their own and some examples are ALOHA, CSMA, CSMA/CD and CSMA/CA. This is a case of contention based channel access. Contention based slots are used when multiple

users try to access the channel at the same time. So the channel is not naturally reserved for any particular user rather, one particular way is that users try to access channel in random manner. There are chances of collision in this but possible remedies are CSMA CD or CSMA CA. In case of collision, there is a retransmission window to retransmit the lost packets and depending upon implementation, it retransmits only the lost packets or the whole transmission window. Some examples of contention based channel access are ALOHA, MACA and MACAW.
[14] [15]

Carrier Sensing

When stations transmit randomly, there is a probability that two or more stations might start sending data at the same time resulting in collision and then the transmitting node needs to retransmit the lost frame. This is basic ALOHA and an added feature is slotted ALOHA in which time is divied into fixed slots, exactly equal to the time required for the transmission of data and nodes must transmit only at the beginning of slots. CSMA stands for Carrier Sense Multiple Access in which every node senses the medium before transmission. There are two types of CSMA implementation i.e. CSMA/CD and CSMA/CA. CSMA/CD is Carrier Sense Multiple Access with Collision Detection in which sender detects the collisions and in case of collision, last sent information will be retransmitted. There are variables like what was the window size which determines how much of information should be retransmitted. Since the information has to retransmitted, it is loss of bandwidth for the lost information packets. CSMA/CD is mostly used in Ethernet protocol since it needs detection of collision on physical cable medium. CSMA/CA is Carrier Sense Multiple Access with Collision Avoidance. CSMA/CA is more efficient in a way that it protects collision from happening in the first place. The way it works is that nodes sense the medium to check if there is any transmission already going on or not. If there is any transmission already going on in the medium, the stations hold their transmission, wait for the going on transmission to finish and then wait for DIFS time period and backoff for a random period and after that, STAs sense the medium again, if the medium is free now, this node will start transmitting data otherwise wait as the process of sensing the medium will be continued. The random backoff time is introduced to cater the possibility that any other station waiting for the medium to get free as well could start transmitting at the same time. There are

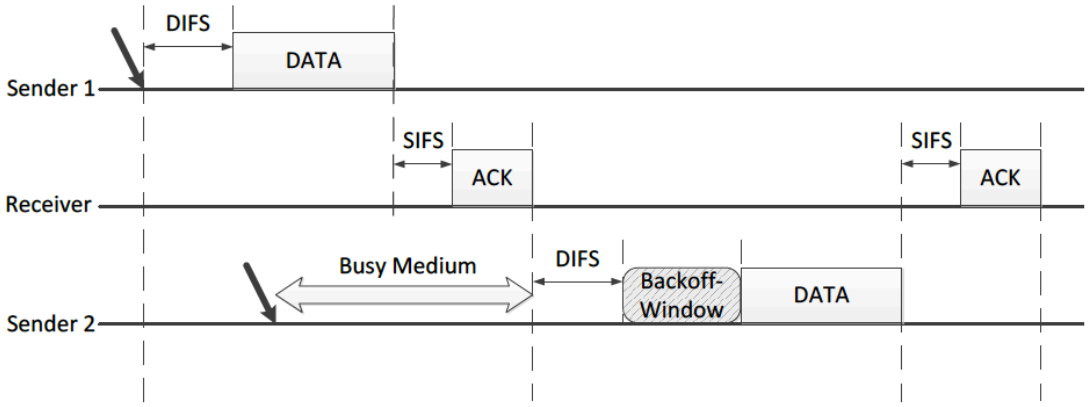
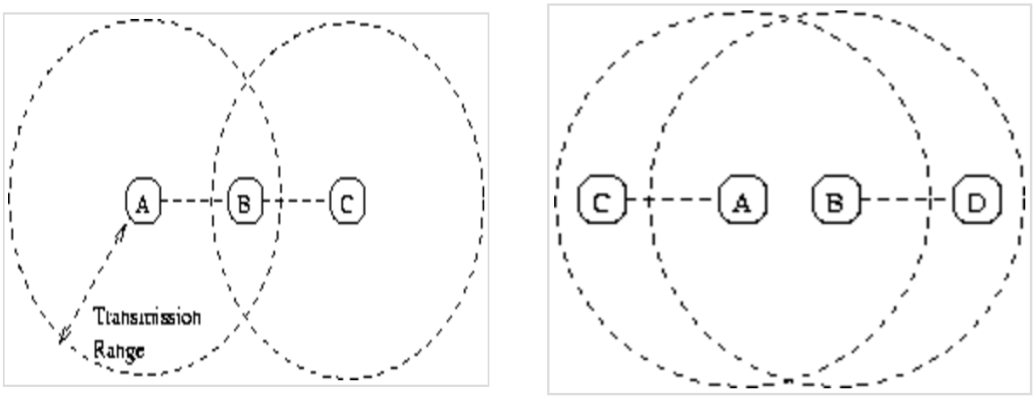


Figure 2.3 *Basic Access mechanism for channel access*

2 main types of data sending mechanisms defined in 802.11 systems. RTS/CTS and Basic Access Scheme. RTS/CTS is better in higher data rate and BER scenarios since it reduces the probability of error by introducing RTS and CTS frames. The function and benefit of RTS/CTS is defined in next section. Basic Channel Access is better for low data rates and sinr related scenarios since it does not introduce much of delay and overhead and hence is efficient in scenarios with less probability of error. The data access mechanism for basic access method is shown in the following figure 2.3

As the 2.3 shows that sender 2 sensed the medium busy while sender 1 was transmitting, sender 2 waited for DIFS and some random backoff period and then sensed the medium free therefore it started transmitting. There are still some problems that need to be solved in wireless channel access. Fig 2.4(a) shows Hidden Terminal problem where nodes A and C are hidden from each other and hence cannot sense the ongoing transmission from each other towards B. Whereas on the right side, there is 2.4(b) which shows exposed terminal problem where A and B are exposed to C and D. Communication from C to A and B to D is still possible since it doesn't intercept each other but as C can sense transmission going on at B, it won't transmit.[16]. [17]

RTS/CTS is another mechanism of channel access using control frames like Request To Send (RTS) and Clear To Send (CTS) to solve hidden terminal and exposed terminal problems, see 2.5. RTS is used by sender node to request the destination node if its available to receive data and CTS frames are used by that destination node to indicate to source node that yes it can start transmitting. These RTS and



(a) (b)

Figure 2.4 *Hidden and Exposed Terminal Problems in Wireless channel access*

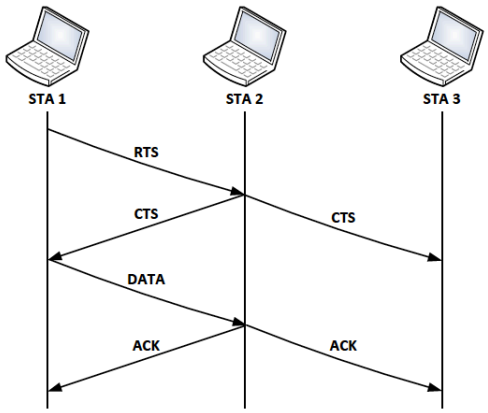


Figure 2.5 *RTS/CTS mechanism for channel access*

CTS frames have information about how long this transmission will take place so any node in the range listening to these RTS or CTS frames can get time information and update their Network Allocation Vectors (NAVs). Network Allocation Vector is a counter which gets filled in according to these sensed RTS CTS frames and when this NAV counter expires (goes to zero), this node starts sening the medium again. After receiving an RTS CTS frame and setting up NAV, node can update NAV when it receives another RTS/CTS/Ack frame accordingly. [18]. This RTS CTS scheme works well in Infrastructure based networks scenarios where as when ad-hoc networks are concerned, RTS CTS adds some additional overhead which reduces throughput and it gets worse as traffic in network increases. [19] Now that we have defined the sensing mechanisms used in IEEE 802.11 suite of protocols, let's

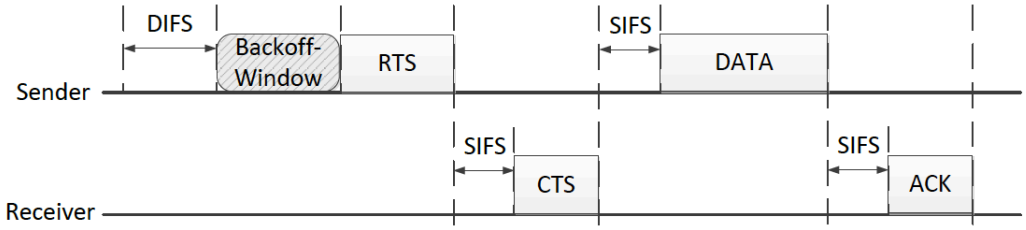


Figure 2.6 *One complete transmission cycle of DCF with RTS/CTS*

take a look at how to access channels in this Wifi suite. Access mechanisms involve specific set of coordinate functions for specific task. Random access schemes use DCF as coordinate finction while PCF is used in schemes like controlled access / taking turns.

2.2.2 Coordination Functions

Distributed Coordinate Function

In random access mechanisms, stations basically decide randomly who will transmit and if there is any collision, stations wait for a random backoff period and then transmission cycle starts again. CSMA/CA along with random backoff period constitutes DCF. [16]. DCF is the mandatory coordinate function used in IEEE 802.11 systems in contention based channel access. A complete transmission cycle of DCF using RTS/CTS access scheme is shown in figure: 2.6

Point Coordinate Function

In IBSS, PCF is used to provide contention free channel access. As this is used in Infrastructure based BSS, AP is usually in control of which stations gets channel access and when.

Hybrid Coordinate Finction

HCF provides Quality Of Service functionalities in Coordinate Functions and can be used in both contention based (Enhanced Distributed Channel Access EDCA)

and contention free (called HCF Controlled Channel Access HCCA) channel access.

Mesh Coordunate Function

MCF is used in mesh BSSs to fully facilitate mesh networking. It can be used both in contention based and contention free channel access.

These coordinate functions use some specific Inter Frame Spacing as described below.

RIFS

Reduced Inter Frame Spacing is space used between multiple transmissions from the same transmitter.

SIFS

This is the Short Inter Frame Spacing, the shortest used in DCF. SIFS is added before every CTS, Data and ACK frame, if RTS/CTS is used.

PIFS

PCF based Inter Frame Spacing is used when PCF is used for contention free slots.

DIFS

Distributed Coordinate Function based Inter Frame Spacing is mandatory in every access mechanism using DCF. The medium should be free for the whole perios of DIFS before a station can transmit.

AIFS

Arbitrary Inter Frame Spacing is used if quality of service is used as described in EDCA. The value of AIFS depends on which class of EDCA is being implemented.

EIFS

In DCF based access mechanisms, if last received packet was eroneous, then EIFS is used instead of DIFS.

3. IEEE 802.11S

3.1 Overview

IEEE 802.11 was traditionally wireless in a way that STAs connected to AP wirelessly but AP's connected to each other and to other technologies using wires. The idea behind it was to get rid of wires on access level but this was only the first step of ease and flexibility. However, it was not too flexible since there were still wires in the backend, so deployment in hard to wire areas was difficult. Moreover, issues like wire breakage and cost were still there. Making a mesh of wires and scaling up gets out of hands because of cost and complexity. In order to solve this problem, IEEE introduced a wireless mesh task group in Jan 4, 2015. [20] The first meeting of this task group was held in July 2015. The main task of this group was to design MAC layer to build wireless mesh Extended Service Set. This mesh was supposed to make wireless connections among APs and also propose an automized way of learning routes for data delivery. This would solve the problem of arranging so many wires, would be cheaper and more flexible. It would still require wire to connect this network to other networks / ethernet.
IEEE 802.11s uses multihop wireless relaying to transfer data from source to destination . Since the network is wireless and a set of protocols were designed to calculate path to destination automatically, it introduced robustness and self healing characteristics in the overall network. Multihop has a drawback of introducing delay, hence reducing throughput in the network. This protocol used its own Mesh Coordinate Function which is described already in chapter 1.

3.2 Use Cases

IEEE 802.11s was and still is very popular for converting wired applications to wireless and here are some examples of cases where 802.11s is useful.[21]

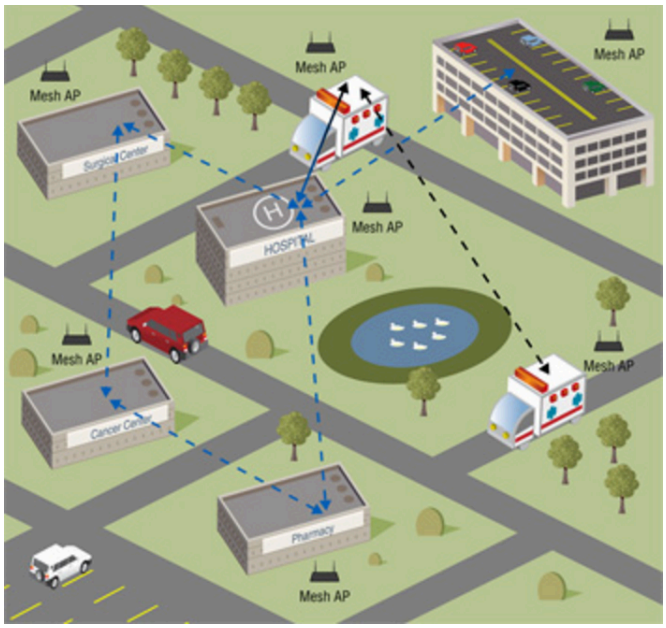


Figure 3.1 *Mesh Network in a public access area.*

3.2.1 Offices

In order for office workers to move around easily while not losing network accessibility, IEEE 802.11s is very useful as it increases the range without imposing much of cost. Also reliability of mesh networks is the key to an office environment with route creation on the go as an added advantage.

3.2.2 Campus / Public Access

Mesh networks can cover a large area which serves the purpose of public internet access. Because mesh networks are quite cheap and they can serve hard to wire and rural areas where wired network is very difficult or impossible so adoption of IEEE 802.11s in public access networks is very common. Fig 3.1 shows mesh network in a public area. [22]

3.2.3 Home Usage

In a typical house hold environment where people own many devices, reliability and tolerance to link failures is key and this is the reason that IEEE 802.11ah is a great choice for home network deployment.

3.2.4 Public Safety

IEEE 802.11s's capability of incorporating ad-hoc device to device based communication to infrastructure mode network makes it more safe and secure for general public. This can also help surveilance activities on common street / crowded areas to protect civilians and residents.

3.3 Devices Used

IEEE 802.11s is a sophisticated set of protocols which includes devices for specific tasks as described below: [20]

3.3.1 Station

Stations are any wireless capable devices which can send and receive data following IEEE 802.11 standards.

3.3.2 Mesh Stations

Mesh stations are stations, capable to tranceive data wirelessly, contributing in mesh network. These mesh stations can also forward data from non mesh wireless stations to the mesh network. [23]

3.3.3 Mesh Access Point

MAP is a mesh AP for stations using this mesh network and also for stations not using mesh network. MAP also establishes peer connections between other MPs and MAPs. So MAP works as an AP for STAs and also as MP for peering with other MPs.

3.3.4 Mesh Point

Mesh Point MP establishe peer links with other neighbouring MPs participating fully in this wireless mesh network.

3.3.5 Mesh Point Portal

MPP is a gateway for this wireless mesh to communicate with other networks e.g. ethernet etc.

3.4 Topology Formation and Protocols

IEEE 802.11s uses routing protocols on MAC layer (on top of Address Resolution Protocol) to calculate routes to end destinations. The purpose of routing table is to learn available routes on an existing network, build routing tables and make routing decisions. [24] On the basis of operation, routing protocols can be categorized as Distance Ventor routing protocols and link state routing protocols. Distance Ventor routing protocols determine the path to the destination based on distance between them and the direction of next hop to reach that destination. DV routing protocol use periodic updates to stay informed about the topology and links in the network. Link state routing protocols in contrast get the information of the complete topology through all the other routers. Updates from other routers are not received periodically instead, in case of a change, the affected router sends update packets to all the other routers in the network. IEEE 802.11s implements proactive, on-demand and hybrid way of topology creation. The protocols used and their procedure are listed below:

3.4.1 Proactive

Routes are created ahead of time in Proactive type routing protocols. This means when the network gets setup, the nodes send request and reply messages and so, get a view of the whole topology of the network. This process makes routing tables in the memory of these nodes, for destinations, before it is even needed.

Optimum Link State Routing protocol

OLSR is one of the examples for proactive routing protocols. It makes a tree like structure while setting up the network. It's operation is such that Root Mesh Point sends a Path EQuest (PREQ) frame to all other MPs which respond with

Path REPly frames PREP. After PREQ and PREP frames, MPs select their route to ROOT MP based on best path metric. In case of a link failure, MPs send PERR frames only downwards in the tree so that other MPs can switch to alternate / backup routes and rearrange the tree structure. Connectivity between links is constantly checked through Hello messages in OLSR. Each node selects the best possible Multi Point Relay (MPR) to localize the broadcasts from its neighbours and to reach its 2 hop neighbours in best possible way using this MPR. The routing table of each node is calculated based on the link state information in the Hello messages. [25]

3.4.2 On Demand

This types of routing protocols generate routes on demand and not beforehand. This means routes are created only when they are needed, its faster to setup because no routes are calculated and saved in memory during the network setup but it also means that when data has to be sent from one place to another, it might take a little longer since the routes to the destination would have to be calculated at this stage.

Ad-hoc On demand Distance Vector

In AODV, nodes can come and go and the routes are calculated from the currently active nodes. There doesn't have to be a predefined structure of topology and so routes are calculated on the go based on whichever nodes are active and whatever topology they are in currently. It takes a little while to get the route since forwards paths are calculated by route reply packets while reverse paths are calculated by route request packets. Meaning that for forward routing of data, route was made based on the replies other nodes sent (backwards) as a reply to RREQ message. When a link breaks, a route error message is sent to other nodes to notify them of this link breakage. [26]

3.4.3 Hybrid

The basic and mandatory protocol in IEEE 802.11s is HWMP, Hybrid Wireless Mesh Protocol which implements Proactive and On-Demand capabilities of above

mentioned routing protocols for path selection process. In this thesis, since this is a comparison with IEEE 802.11ah where nodes are mostly static and not mobile, we don't really need On-Demand routing protocol so we will focus on Proactive part of HWMP.

3.5 Path Selection and metric

In the network, if proactive links are found, those are preffered for being more stable and reliable. But, if proactive links are not present, nodes then look for on-demand links / routes to the destination. Since we are focusing on proactive part in this thesis, the path selection process for proactive routing protocol OLSR is like this: if node A is looking for path towards node D, node A will send PREQ frames to all nodes in its range. If the nodes receiving these PREQ frames don't have any information about the destination MAC address, they will ignore this message, otherwise the receiving node of PREQ message will send the details of interface and link to the destination with PREP message. [21]
Since this mesh network infrastructure uses a routing protocol to forward packets, there has to be a metric to decide which path is best towards a given destination. Metric are some defined parameters which decide a value and based on that value, routing protocol decides which path to select and place in the routing table. IEEE 802.11s has many routing protocols however HWMP is mandatory, which in itself has many routing protocols. We are considering here Proactive mode of HWMP in IEEE 802.11s and that uses Radio Aware Optimum Link State Routing protocol. IEEE 802.11s does not specifically define any metric but we will consider OLSR's metric here, so the metric (airtime metric) for RA-OLSR is based on Estimated Transmission Count ETX. Nodes send probes in forward and reverse directions at any time T and ETX would then be the fraction of number of probes sent in forward (nf) and reverse (nr)directions as shown in 3.1

$$1/(nf + nr) \tag{3.1}$$

The smallest ETX value link would then be chosen as best path for that neighbouring node. [27] [28]

3.6 Setting up a Mesh network

The complete procedure of setting up a Mesh network is described in [29]. Mesh Discovery, Peering among Mesh Points, calculation of routing paths and creating routing tables are some important factors.

3.6.1 Mesh Discovery

Nodes can discover mesh either via active scanning or passive scanning. Mesh nodes send beacon frames periodically and also there are Probe Response frames sent after receiving a Probe Request frame. These frames contain a Mesh ID for identification purposes. There is also a mechanism for avoiding collision of beacon frames called Mesh Beacon Collision Avoidance MBCA.

3.6.2 Peering Agreements

Mesh Points can communicate to neighbouring Mesh Points only after peering agreements have been established. There is a 2 way handshake mechanism for peering during which each node agrees on parameters that would be used by peer nodes.[21]

3.7 Simulations

3.7.1 Simulator Settings and Parameters

The physical radio used here was IEEE 802.11g at 2.4GHz with 20MHz bandwidth and 52 OFDM subcarriers used (48 for data and 4 for pilot) out of 64 total with each subcarrier spanning over 0.3125 MHz bandwidth. The simulations were carried out for outdoor scenarios using transmitter power as 2 mW, thermal noise -110 dBm, Sensitivity -85dBm and path loss alpha as 2. All the simulations below use the same calculations. The antennas at transmitter and receiver side are not adding any gain so gains are 0.

3.7.2 Code Validation

There is a greenie protocol introduced in Euracip Journal for Wireless Communication and Networks JWCN by Alfonso Araisa Quintana which implements proactive,

reactive (like on-demand) and hybrid ways of routing for video data streaming over wireless mesh networks [30]. The code was written in C++ for omnetpp simulator and implements proactive part of routing just as mentioned in IEEE 802.11s. We integrated this implementation in our coding environment to test the validity of code and since it follows IEEE 802.11s's proactive routing part, it serves our purpose of checking routing efficiency and throughput of this protocol in pre-established network. This section describes the simulation scenario, simulator setting and results obtained by this implementation.

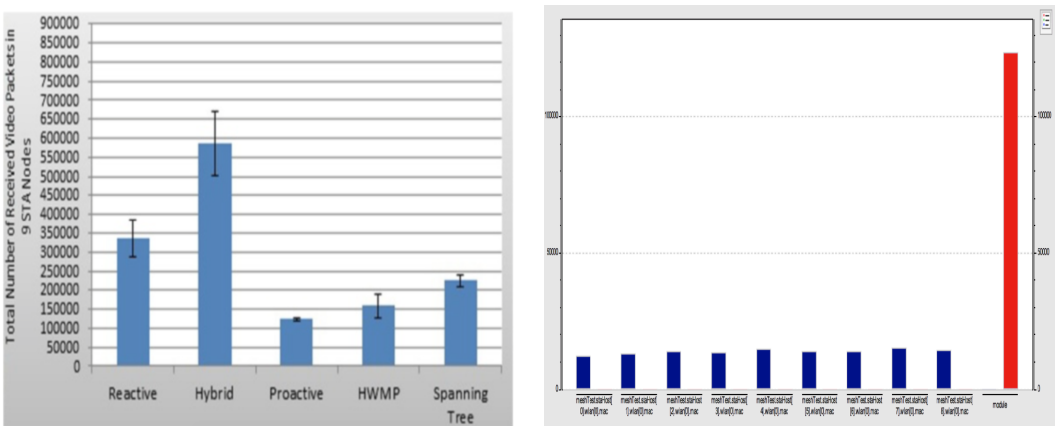
In this simulation there are 5 MPS, one of them is working as server and the rest are forwarding traffic to this server. The STAs connected to MAPs and then to MPs act as clients and request video streams from the server. As this video stream can reach client from any MP or MAP, the paths followed are different which brings felxibility and self healing characteristics to the network and that being the reason of choosing IEEE 802.11s underneath as base protocol for this GREENIE protocol.

Traffic interval is such that 512 MB of data packets are sent every 0.08 seconds and the total data size is 10MiB. Since video packets are used so Constant Bit Rate, CBR, streaming model is used. EDCA is used for channel access.

The Proactive protocol works in such a way that when a node receives a packet, it checks the destination address in its routing table, if the destination network is listed in its routing table, this node will then check the exit interface that leads to that network and forward the packet on that interface.

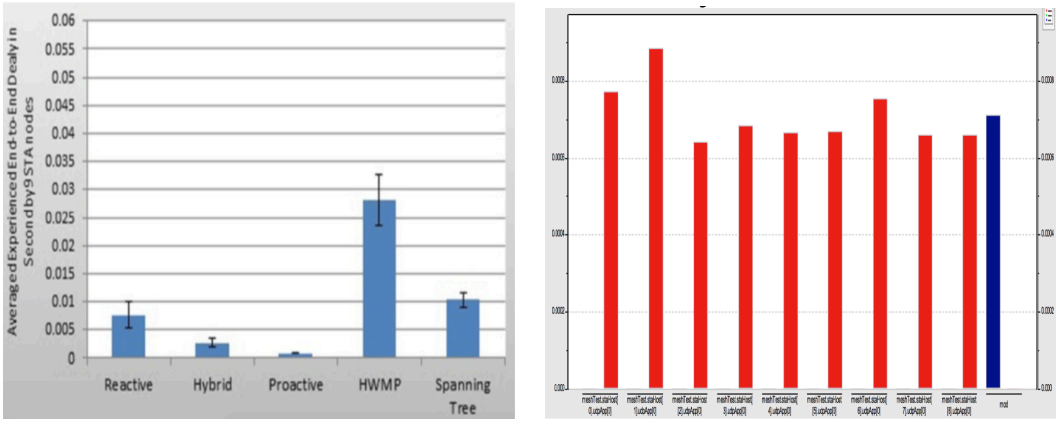
This protocol is implemented using INETMANET framework in OMNETPP. [31] In first scenario, STA nodes were requesting video streams from the server and all other nodes were relaying data from server. The efficiency criteria was number of Bytes sent successfully and routing overhead. In the results diagram below, the one on the left,3.2(a), was the one displayed in the journal showing that about 125,000 packets were received using Proactive protocol [30] while on the right are the ones simulated for this thesis 3.2(b).

In both cases, the total number of video packets received by STA nodes were about 125,000 in 5 runs in average. 3.3(a) shows the results for end-to-end delay for the same configuration as stated in [30] which appears to be little less than 0.001



(a) (b)

Figure 3.2 *(a) results of Greenie's implementation. (b) results obtained in TUT ELT dept implementation*

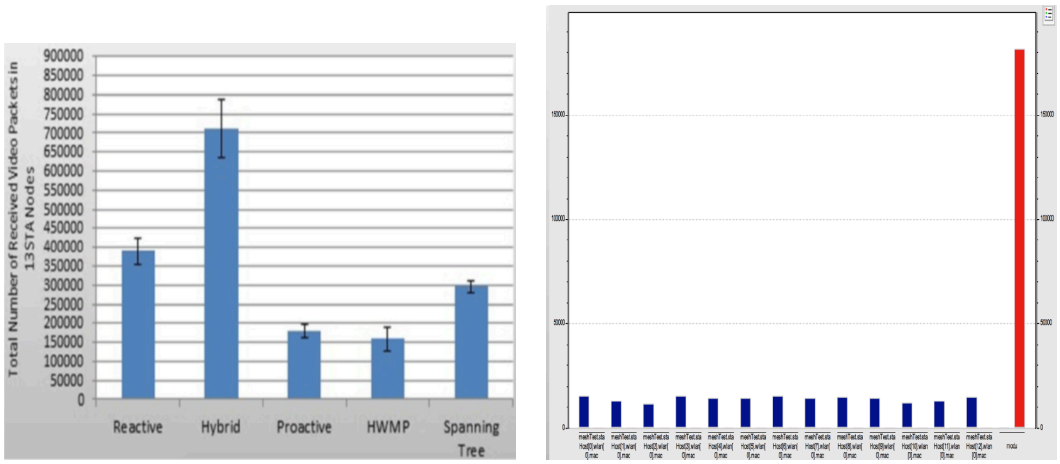


(a) (b)

Figure 3.3 *Average end-to-end delay in 9 sta nodes, (a) results of Greenie's implementation. (b) results obtained in TUT ELT dept implementation*

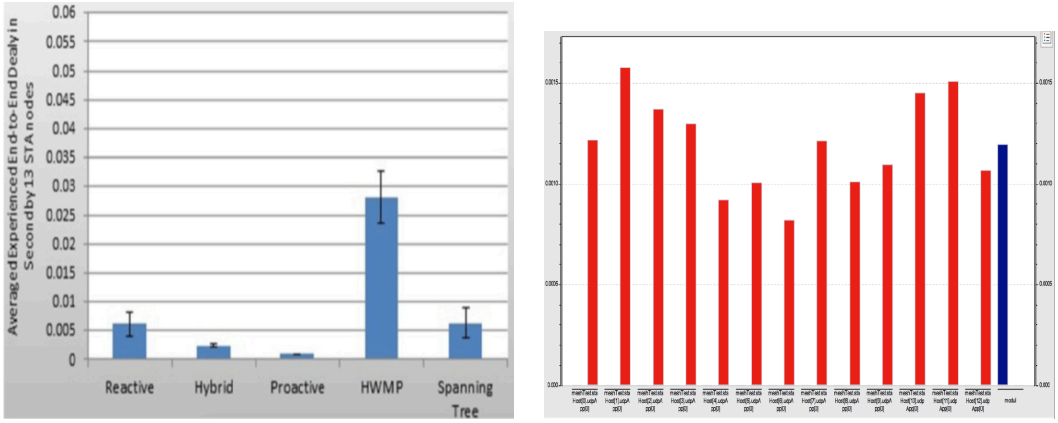
seconds while 3.3(b) shows the results from simulations performed for this thesis in TUT ELT Dept and the end to end delay reulted in 0.00071 seconds..

The same configuration was performed once again for 13 nodes in 3.4 where 3.4(a) represents the total number of packets received in journal's simultion while 3.4(b) was the total number of packets recieved by 13 nodes in our simulation in 5 averaged runs. In both simulations, the total number of packets received nodes in average came out to be about 175,000. While 3.5 shows the end to end delay of same



(a) (b)

Figure 3.4 *(a) results of Greenie's implementation. (b) results obtained in TUT ELT dept implementation*



(a) (b)

Figure 3.5 *Average end-to-end delay in 13 sta nodes, (a) results of Greenie's implementation. (b) results obtained in TUT ELT dept implementation*

configuration as Greenie's graph is on left while on right is from TUT dept. Notice that in TUT ELT simulations, blue bars represent individual nodes' data while red bars represent averaged data.

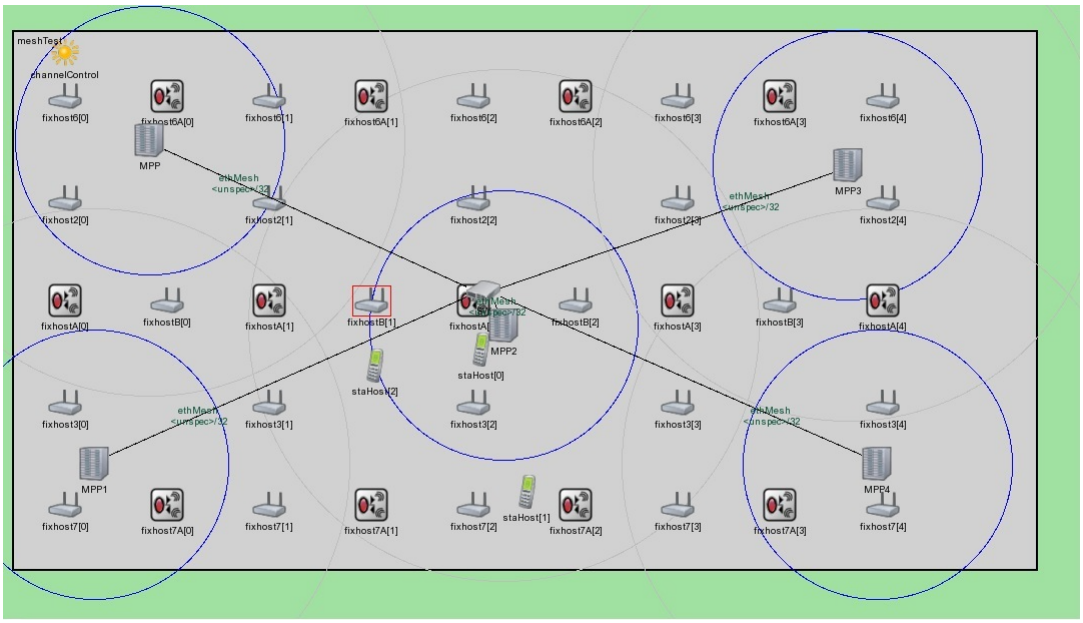


Figure 3.6 *Simulation topology*

3.7.3 Simple Scenario, no mesh host

In this section, we would take a look at the throughput of the above mentioned scenario. We removed the mesh host part of the above simulation scenario. Since it was tested and results were found correct, further tweaking of the same simulation scenario would also reveal correct results. In this simulation scenario, mesh hosts were removed from the network and there were only station hosts, mesh AP relay, basic mobile manet mesh and MPPs as shown in figure. 3.6 . Since this is infrastructure mode, OLSR is working in these nodes to create routes form Station host to destination MPP and all the devices in middle act as relays to transfer data. The simulation is run for 30 secs.

Data Flow

The hierarchy of data transfer is such that MPP2 sends data packets to Swicth which is in turn connected to MPP (0, 1,2 and 3). These MPPs then transfer those data packets to Mesh Portals , then to Mesh Relay APs and finally station host connected to APs receive the data. Bear in mind that OLSR has its own MultiPoint Relay which is chosen based on some parameters. So the AP or Mesh Point whichever

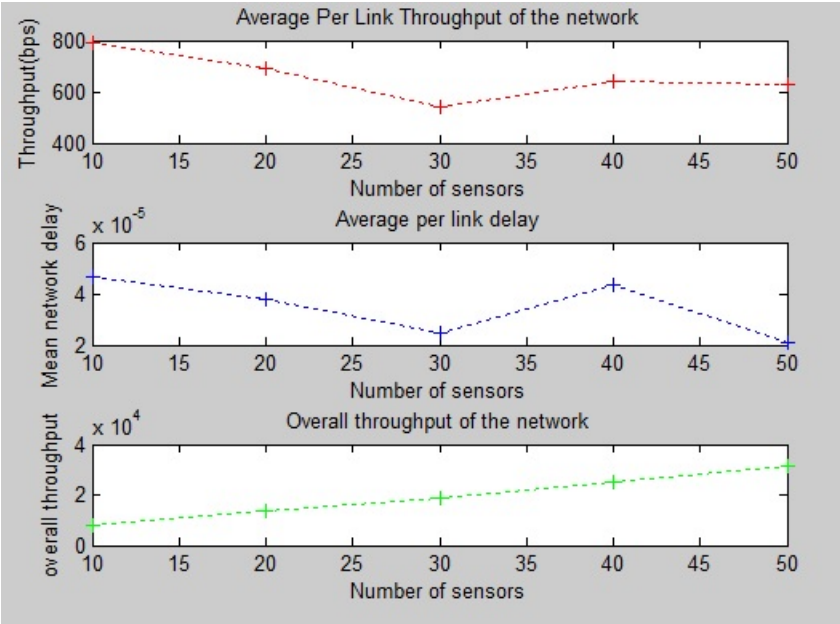


Figure 3.7 *Average per node throughput, delay and overall throughput in IEEE 802.11 s simulation with 10 , 20, 30, 40 and 50 stations*

would fulfill those criteria of OLSR would be selected as MPR and would relay data to station host. This MPR selection is different for every simulation as this is based on link metric and also nodes location in all scenarios is random within the defined playground. Below figure 3.7 shows the average per node throughput of 10, 20, 30, 40 and 50 station hosts. Also the end to end delay for those station hosts is shown in the same figure. Overall throughput of the network is total number of bits sent and received by all stations divided by total simulation time, so if some nodes are not receiving data for the time being and are idle, the overall throughput would be less accordingly and same goes for the delay as delay is the mean delay of nodes sending requests and receiving data.

Although overall network performance in mesh works on best path possible, so some far away nodes might have only one good path and the throughput for that path depends upon the quality of link. So its fair to say that performance of mesh network depend heavily upon the topology and network links, far away nodes result in less throughput towards the network. But for the most part, performance of mesh network is usually better than other protocols because of multiple paths availability and best path selection for routing. Also the path selection is autonomous so setting up the network is really easy.

3.8 Performance

The performance of IEEE802.11s can be seen from the throughput graph. Depending upon the scale of network, IEEE802.11s performs pretty nicely but there are some cons of this technology:
1. Because of IEEE 802.11 g as physical radio, range of communication is still about 100 to couple hundred meters, (depending upon inout power, B.E.R, SNIR, Gains and Noise Figures of transmitter and receiver). In our simulations, the range was 140 meters without the relay. This means, we have to use relay, eith MAP or MP avery 120 meters or so .
2. Because mesh stations are also relaying data sourced from or destined to other stations, some nodes / links may get extra traffic just to pass through and that introduces unnecesssary delay in processing of their data and also the throughput for data originated from this relay node decreases. This is one of typical problem in multi-hop relay networks
3. Because of using multi-hop relay in the networks, some links can be overcongested sometimes untill the next hello packet flows in the network telling the nodes about the link condition. So for small instances of time, some nodes can be overcongested and some can be free. This can however be rectified by reducing Hello timer, there would be more Hello packets flowing in the network then but those would still introduce less overhead and congestion than big data packets.

4. IEEE 802.11 AH

4.1 Overview

4.1.1 Introduction of IEEE 802.11ah

Since the amount of devices owned by a regular person these days is increasing enormously and along with the advent of social networking, these devices want to communicate to each other on a regular basis and in an automatic fashion. It is predicted that the amount of these connected devices used by people would go up to 38.5 billion by 2020.[32] The confluence of emerging small sized electronic devices and high speed network connectivity paved the path of "Internet of Things" concept as we know it today. [33] In order for these devices to communicate unanimously and coherently, a standard protocol is needed to be used world wide by manufacturing companies and service providers. These devices mostly operate on batteries so energy efficiency and range of communication is also a strong concern. IEEE SA assembled a Task Group called ah which had their first meeting in 2010 to solve this problem [34]. The main task of the group was the standardisation of a protocol for small battery powered sensor devices. The protocol is supposed to work with pre-existing applications so IEEE envisioned it as one of the WiFi group of protocols and hence only layers 1 and 2 of OSI reference model would be proposed while the rest of layers would work as normal. The communication model for this protocol is envisioned to work as both device to device communication and also device to gateway. Technically, .11ah is 10 times downclocked version of IEEE 802.11ac so there are some phenomena similar as in .11ac . The outdoor path loss model for IEEE 802.11ah is derived from IEEE 802.11ac. Because of sub GHz operating frequency, the range covered by devices using this protocol is quite long (dicussed later in this chapter).

4.1.2 Phy layer modification

In real world, physical layer deals with bit level transmission of data in physical medium (either wired or wireless) and so the modulation and coding schemes for these bits to be transferred, channel model and path loss models are discussed in this section. IEEE802.11ah's physical layer is designed to efficiently enhance transmission range while providing minimum 100 Kbps bandwidth. The operating frequency channel is licence exempt sub 1Ghz frequency spectrum. More specific channels for this protocol used in different countries are listed in Table 4.1: [35].

In this thesis, we are focusing on USA frequency model which gives us 26MHz

Table 4.1 *Sub 1 GHz bands applicable for IEEE 802.11ah in different countries.*

Country	**Frequency Range (MHz)**
China	755 - 787
Europe	863 - 868
Japan	916.5 - 927.5
Korea	917.5 - 923.5
USA	902 - 928

between 902 MHz to 928 MHz. As mentioned earlier, some of the features in IEEE802.11ah are similar to IEEE 802.11ac. In case of bandwidth, 802.11ah is 10 times downclocked version of 802.11ac so supported bandwidths are 2MHz, 4MHz, 6MHz and 8MHz. There is one more 1MHz bandwidth channel introduced in .11ah for extended range purposes having slow data rates using MCS 10. This mcs 10 is new in .11ah which is not from .11ac. [35]

Modulation and coding schemes

802.11ah uses OFDM signals for wireless transmission and these signals are codded using Binary Phase Shift Keying , Quadrature Phase Shift Keying, 16-Quadrature Amplitude Modulation (QAM), 64 QAM and 256 QAM. The data rates achieved by these codings depend on bandwidth, number of spatial streams used, guard interval and coding rate. Ofcourse energy utilized would be higher if higher modulation schemes are used. Throughout this thesis, we are using 2MHz as bandwidth, single spatial stream and 8us as guard interval. The coding rate, corresponding data rates

and SINR achieved are shown in the table 4.2. Based on these values, sensitivity can be calculated as shown in equation 4.1, which is the minimum signal power needed for the signal to get detected and be decoded as data. In the equation, S represents sensitivity, N is noise power and Sinr min is minimum Signal to Interference Noise Ratio required .

$$S(dB) = N + Sinrmin \tag{4.1}$$

Note that this is the equation in dB, that is why Noise and SINR are being added. In regular scale, these parameters would be multiplied as shown in chapter 2. Required SNIR, and other parameters result in data rates as shown in table 4.2. CR here represents Coding Rate, DR is data rate, N bpscs is number of coded bits per subcarrier per spatial stream, N cbps is number of coded bits per symbol and N dbps is number of data bits per symbol. [16]

Table 4.2 *MCS and Data Rates for IEEE 802.11ah.*

Index	**Modulation**	**CR**	**N bpscs**	**N cbps**	**Ndbps**	**DR (Kbps)**	**SINR**
0	BPSK	1/2	1	52	26	650	11.41
1	QPSK	1/2	2	104	52	1300	14.45
2	QPSK	3/4	2	104	78	1950	17.12
3	16-QAM	1/2	4	208	104	2600	20.39
4	16-QAM	3/4	4	208	156	3900	23.76
5	64-QAM	2/3	6	312	208	5200	28.18
6	64-QAM	3/4	6	312	234	5850	29.76
7	64-QAM	5/6	6	312	260	6500	30.89
8	256-QAM	3/4	8	416	312	7800	36.09

Path loss models

Maximum transmitter power in ISM band is 30 dB / 1 Watt without antenna gain. [36]. IEEE 802.11ah can be implemented indoors and outdoors. Indoor model follows IEEE802.11n's path loss model while outdoor path loss models are based on 3GPP spatial channel model which supports MIMO and SISO radio links [37]. We are only considering SISO here in this thesis. Within outdoor deployment models, there are Macro, pico and device to device based deployment scenarios but we are only considering macro path loss model here, as shown in equation : 4.2

$$P.L = 8 + 37.6log10(d) \tag{4.2}$$

This equation is taken at frequency 900 MHz where d is in km. The antenna height in this case is 15km above rooftop level and the path loss exponent comes out to be 3.76.

Link Budget Analysis

Referring to Link Budget Analysis figure 2.2 shown in chapter 2. We are considering transmitter power to be 1mW. Feeder losses and gains are assumed as 0 dB, although antenna losses are quite less as compared to gain of antennas in real life. Friis Transmisison Equation is used to find the received power at the receiver antenna in free space and is shown in equation: 4.3 taken from [38].

$$Pr = Pt * Gt * Gr * (\lambda/4.\pi.R)^2 \tag{4.3}$$

Here Pr is received power at receiver antenna, Pt is transmitted power, Gt and Gr are transmitter and receiver antenna gains respectively and R is the distance in meter. If we convert the mentioned equation for R and change the units to dB scale, the equation takes the shape as shown in: 4.4

$$Pr = Pt + Gt + Gr - Lp - Lt - Lr - Lm \tag{4.4}$$

Lp is the path loss, Lt and Lr are feeder cable losses for transmitter and receiver respectively and Lm are misceleneous losses (whose major portion is fading loss). The recommended value for Lm is 15dB . Note: if fading losses are calculated in path loss model already or in sensitivity calculations, we will not use them again seperately here. With 1mW as transmitter power, the range comes out to be 170 m.

Modelling of Phy layer in Simulator

We will discuss the details of simulator and how it works in detail in chapter: 6. But for now, some basics about phy layer modelling in the simulator are described

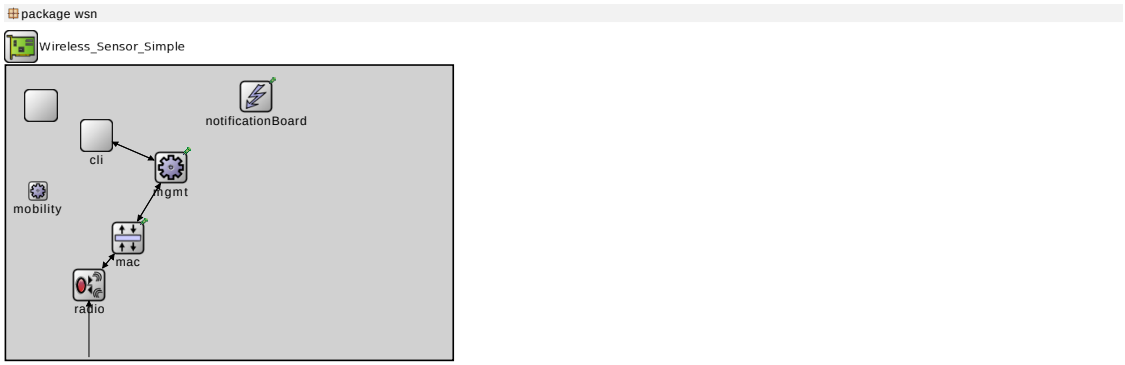


Figure 4.1 *Station module modelled in omnetpp containing management, mac and phy layer sub-modules*

in this section. The module that handles Phy layer is described in figure: 4.1 This figure explains the different layers in Station module i.e. radio, mac and management submodules, but if we dig deeper in radio module, it contains radio.cc and radioModel.cc as code files which explain what this module is supposed to simulate. In those files, we initialize the radio module, which works at 900 MHz center frequency and 2 MHz bandwidth, we define the transmit and receive states of radio module. How a radio is supposed to handle the messages is also defined in these files, e.g. if radio receives a data packet, we have this function (isReceivedCorrectly) in code which sets some pre-defined SINR values for different mcs schemes. These values were given to us for this thesis after validating in another simulation. We have channel of IEEE 802.11ah modelled in IEEE80211ChannelControl.cc which basically employs path loss model described above in 4.2. So when the transmitted signal travels through this channel, it gets deteriorated in strength based on the path loss model, which basically means noise and interefernce affects the transmitted signal and dampens it. Then we have function (isPacketOK) in radio model code which will check if the received SINR is less than or equal to threshold SINR, then it will discard the packet and display that the noise was too much so package could not be decoded successfully. Otherwise, if the received SINR is greater than threshold SINR, we assume that this packet is received correctly and we transfer it to upper layer. The piece of code for this task is attached in Appendex A.

4.1.3 MAC layer modification than 802.11

IEEE802.11ah MAC is quite different from other IEEE 802.11 MACs because of sub 1 GHz physical layer and also some MAC features introduced in .11ah are peculiar in this protocol for saving energy, enhancing range of communication and affording thousands of sensors in one AP. These features are referenced from [39] and described below:

Enhanced Distributed Channel Access

DCF and PCF are both basis of HCF called Hybrid Coordinate Function. EDCA is a type of HCF which provides contention based prioritized access while using CSMA/CA for carrier sensing . EDCA introduces Arbitrary IFS and high priority traffic gets less AIFS which means they have to wait less time to sense the medium again and transmit if medium is found free also the backoff timer for high priority station is also less. Whereas low priority stations have more AIFS value and hence have to wait longer to sense the medium and ofcourse if the medium is busy, this station would have to wait for a longer backoff time and then start sensing again. [40]

Auto Rate Fallback

There are fading, attenuation, nearby transmissions and moving objects etc in Wireless Communication and so the performance cannot be guaranteed. To cater this, there is a mechanism called ARF in IEEE 802.11 systems. The way it works is that if 2 consecutive transmissions fail, it means there is an error due to collision or anything. Hence, the sender reduces the rate of transmission to next available lower data rate. However, if 10 consecutive transmissions are successful, the sender sends the next packet with one step higher data rate available and if it gets an acknowledgement for this transmission, this data rate is adopted. Otherwise (in case of collision) the data rate is lowered back to last used data rate. [41]

Random Access Window

STAs try to send RTS packets (in case of RTS/CTS) or data (in case of Basic Access mechanism) as soon as they receive beacons, Now if there are thousands of STAs in the communication range, it makes chances of collision a lot more. RAW limits channel access to small number of STAs at any particular time and hence spreads this uplink communication (from STA to AP) attempts over a longer period of time. STAs extract the time slot when they should start transmission from RAW information privided in the beacon that they receive from the AP. [42].

Target Wait Time

TWT essentially manages STAs' transmissions by scheduling them in different time slots. STAs requesting for TWT slots are called TWT resquesting STAs and the STAs that respond to TWT requests are called TWT responding STAs. AP's can also respond to TWT requests. According to the standard, TWT can be requested by setting the dot11TWTOptionActivated field equal to 1 and will also set TWT requestor support field equal to 1. The same goes with TWT responding STAs to have dot11TWTOptionActivated and TWT responder support fields equal to 1. [16].

Frame Structure

There are many options in IEEE 802.11ah regarding MAC features and those all are based on subfields in control frames. As those are optional, only the general frame format for MAC header in IEEE 802.11ah is shown in 4.2. In this frame structure, the first 3 fields, Frame Control, Duration/AID, Address 1 and last field FCS are necessary in every frame. The rest address fields, sequence control, QOS, HT and frame body are optional.

Frame Control

Frame Control has in turn, many sub fields. The value to those subfields define fragmantation, power management, to or from DS and other features like retry number etc.

Duraiton /AID

This Duration field helps other stations listening on the same channel to adjust their NAVs for how long the curent transmission will continue. The AID number is the Association IDentifier of the STA which is cuurently transmitting this packet.

Address

Address fields are to identify the source and destination addresses of BSSID and transmitting station. But here in this case where only necessary fields are stated, this address field is the destination STA address for which this packet is intended.

Sequence Control

This field is for keeping track of sequence number of messages/packets in order to find duplicate messages/packets.

QOS Control

This field gives info about the QOS policies implemented.

HT control

HT Control field tells about the link adaptation, MCS used and antenna configuration. The value in this field helps keep adapting to wireless channel irregularities and this value is very important for ARF.

FCS

Frame Check Sequence states the 4 Byte CRC checksum for the frame in order to make sure that the frame was not corrupted in between the transmission and reception.

Bytes: 2	2	6	0 or 6	0 or 6	0 or 2	0 or 6	0 or 2	0 or 4	0-7959	4
Frame Control	Duration /ID	Address 1	Address 2	Address 3	Sequence Control	Address 4	QoS Conrol	HT Control	Frame Body	FCS

Figure 4.2 *Fields of General MAC Frame in IEEE 802.11ah*

TXOP

Transmission Opportunity TXOP is a time interval in which an STA is allowed to transmit as many frames as possible within the allowed duration. This gives a chance to STAs using low data rate (because of higher distance from AP or noise etc) to access channel and compensate somehow for their low data rate since more frames are transmitted all at once in this time duration. STAs that are not authenticated to an AP do not operate in TXOP during RAW.

MAC layer modelling in Simulator

MAC layer model in this simulations checks if the packet received from PHY layer is actually intended for this machine or not, if yes, then it keeps it and performs further actions and sends it to management layer, otherwise MAC layer discards the packet. This checking is based on MAC address in MAC layer and in case of Relays, IP is also checked and those IPs are assigned manually. So STA is simulated to only connect to Relay's ip address and Relay is only associated to final AP's IP address. The mac layer implements DCF ans RTS / CTS in this simulation model. The code file is quite big so instead of attaching the whole file, we will mention here the tasks that are modelled in MAC layer: 1. it checks if the data provided by upper layers is of normal size, the threshold is 2346 Bytes, fragmentation is not currently supported in this simulation model so if data received from upper layers is greater in size, we discard the packet. In our simulation, the packet size is mere 256 Bytes so there is no chance of data getting discarded because the size is quite less than threshold.
2. MAC layer gets the data from upper and bottom layers and adds / removes headers and makes layer 2 frames.
3. Link adaptation as described in section 4.1.3, ARF also happens in this MAC layer.
4. As mentioned, DCF and RTS/CTS are implemented in this layer in code and description of how they work is in section 4.1.3.

4.2 Use Cases

.11ah is a protocol designed to meet a lot of different use cases. Not only it supports IoT devices but also automation and healthcare industries would benefit with this proticol. [33] [43]. While some of them were rejected but among the ones that got accepted, the 3 broad categories are:

4.2.1 Sensors and smart meters

In today's technological world, there is a trend of using smart devices and sensors. The target audience, in case of sensors, is basically in every walk of life. Almost every department, whether in professional companies, sales, research or teaching institutes, uses some sort of sensing, monitoring or tracking in their every day work. An interesting study of social sensors where sensors collect data about individuals' input in community and analyse the benefits / shortcommings can be read at [44]. All these sensing / tracking devices need to communicate to each other or to some central monitoring device. This communication may be periodical or on demand but the critical part here is that the communication has to be unanimous. Resultantly, to cater this increased demand of connectivity, most vendors of low power sub 1GHz sensor devices came up with their own implementation each. [45] This creates an interoperability issue but thanks to IEEE 802.11ah all vendors can now agree on same communication protocol to work in such situations. Some examples of such smart meter technologies are:

Smart Grid

In electricity distribution industry, monitoring electricity usage and hence saving energy is getting popularity these days since it lets load balance power threfore provides efficient supply in the whole neighbourhood. This kind of applications need some protocol with high coverage range and even less data rates (100Kbps) can work and so this is one good example of how smart meters can use IEEE 802.11ah protocol (which supports large number of sensor devices with one AP and data can be communicated with flexible data rates with minimum of 100 Kbps) and communicate with each other when and where energy is needed. The same ideology can be applied to other smart meters like gas and water meters. Figure 4.3 shows IEEE 802.11ah being used by such smart meters. [46]

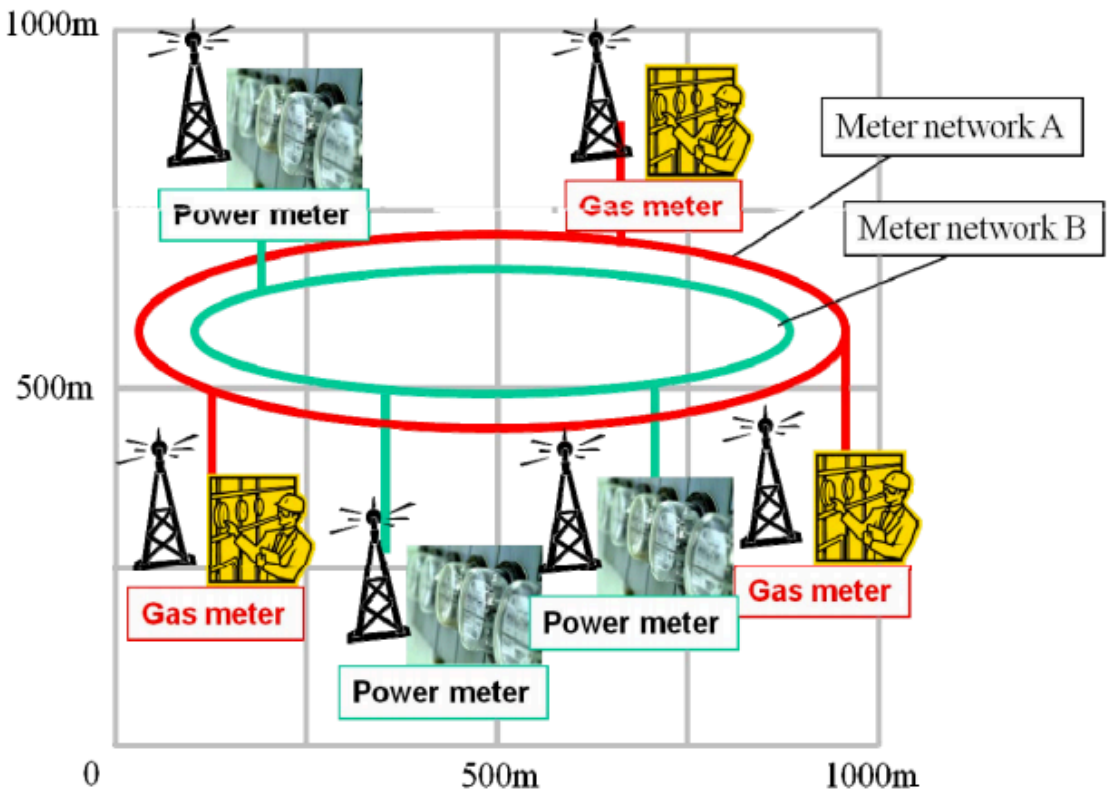


Figure 4.3 *Smart Grid Network.*

Automation

Be it home or factory automation, having anything automatic is only possible if we have sensors sensing something and then the systems acting on the information according to the design. In factory automation, huge machines are being controlled and the results are analyzed based on some predefined protocol. While in home automation scenario, either small devices are being controlled based on some sensor data and actions are performed based on that data or user sends some signals to those machines using some sensors, and the devices act accordingly (e.g. turning any machine/device on or off via a web app/mobile app wirelessly). In all these cases, having small sensors for automation purposes is extremely crucial and the below figure 4.4 shows how IEEE 802.11ah can help in these situations.

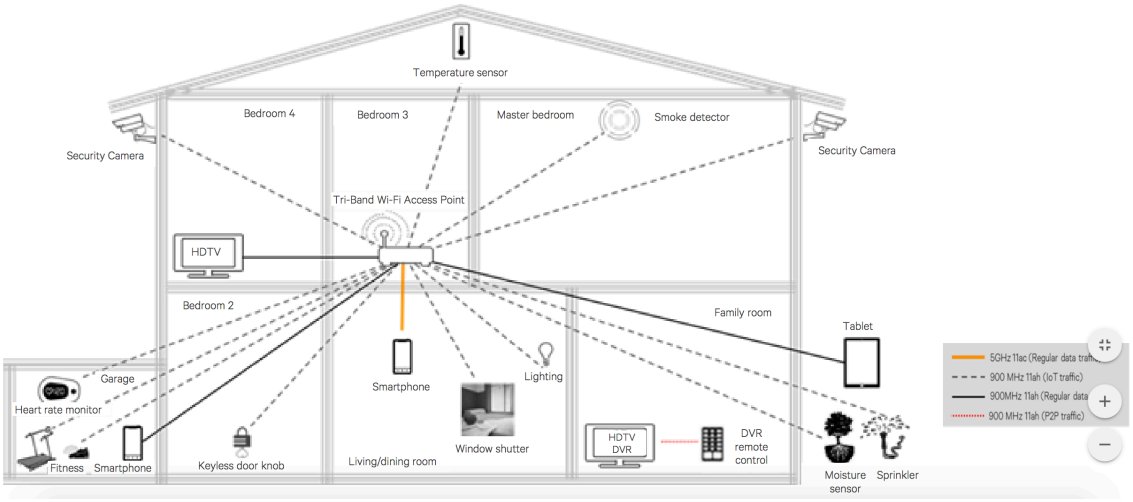


Figure 4.4 *IEEE 802.11ah used for home automation*

Healthcare

Since the range of IEEE802.11ah is quite long (upto 1 km) and one AP can associate thousands of STAs, this nature of IEEE802.11ah makes it fasible to be used in disastrous situations during war. Also sensors connected to vital organs of a human bieng communicate crucial information about the performance of that organ which should be transmitted urgently to Hospital Staff / Doctor / Care taker of patient. IEEE 802.11ah provides a way for all such communications.
Healthcare is one of the most important fields of study and with the advent of technology, small wearable devices can now advance physical as well as mental health of humans. With these wearable devices telling humans how much they ran today, what is their blood pressure and glucose level etc they still need to communicate in a predetermined manner, agreed by all the vendors of such devices.

Internet of Things

Smart meters, sensors, wearables and all such communication devices combine and contribute to this whole Internet of Things , IoT, phenomenon. The internet as we know of today consists of hardware and software, client and server devices communicating to each other.Hence the word Things explains these digital devices as any thing that can communicate. The concept behind IoT is that in near future, almost every digital device would be communicating just like in current internet. (almost

50 billion by 2020 as estimated by Cisco [32].

4.2.2 Backhaul Links

IEEE802.11ah can be used as backhaul for other technologies like IEEE 802.15.4 and IEEE 802.15.4g which means that .11ah can coexist with such technologies. The way it works is that sensors using 802.15.4 or 4g would gather the data and send to 802.11ah STAs which in turn would send the data to 802.11ah AP to be sent to the internet. Figure 4.5 (taken from [47]) shows IEEE802.15.4 sensors using IEEE 802.11ah as backhaul. [48].

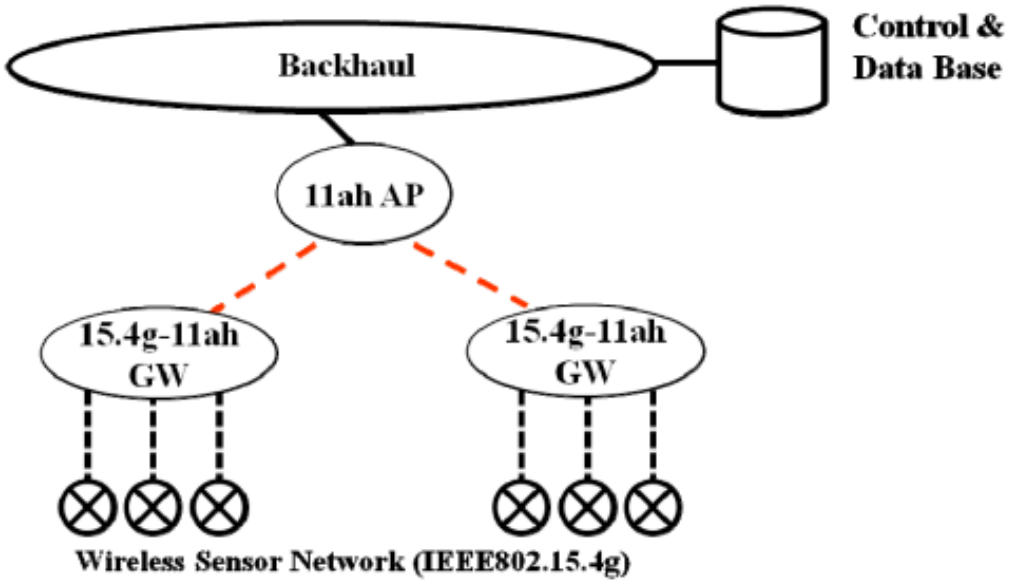


Figure 4.5 *IEEE 802.11ah used as backhaul for IEEE 802.15.4/4g*

4.2.3 Extension in range for WiFi

4.3 Devices Used

The devices used in IEEE 802.11ah are STA, Relay and AP. [39].

4.3.1 STA

STAs are wireless devices which can be the source or destination of data. They are used in both infrastructure based and non infrastructure based architectures. Stations are very peculiar in IEEE802.11ah as they work on sub 1GHz frequency band so Phy and MAC layers are different than other IEEE 802.11 protocols. According to IEEE 802.11ah protocol, STAs must support 1 and 2 MHz bandwidth channels and single spatial streams at radio level.

4.3.2 Relay

Relays are the devices that forward the data from Source towards destination and act as a relay in between. Relays don't open up the packet to look at the data as its not intended for them, their task is just to forward the data to AP towards destination. Relays in IEEE 802.11ah consist of 802.11ah (STA and AP) in such a way that source STA sends data wirelessly to Relay AP, which is connected directly to Relay STA and this Relay STA in turn forwards that data to AP.

4.3.3 Access Point

Access Point is the device which connects the local 802.11ah network to outside network. Outside network could be the internet or other 802.11ah networks. APs also possess the properties of STAs.

4.3.4 Simulator Settings

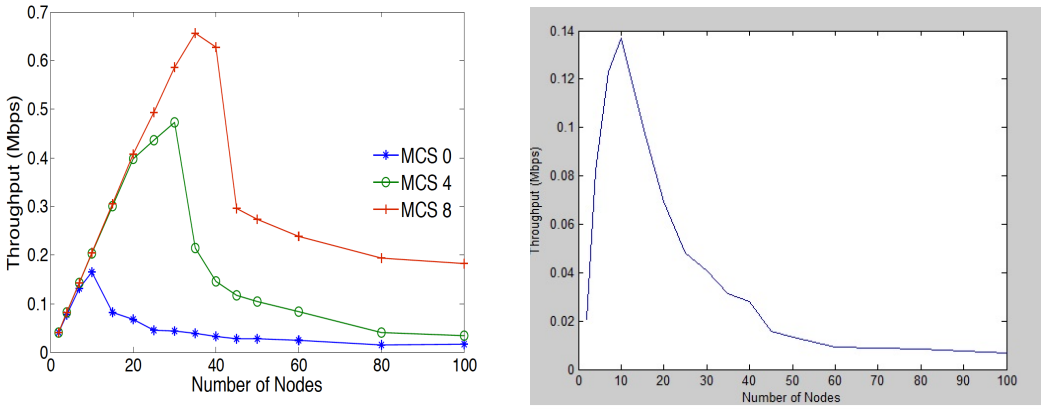
There are some parameters to be given to these simulations and which will remain constant throughout all the below scenarios for IEEE 802.11ah as shown in 4.6. In this figure, Tsym is symbol duration, mshort and mlong are short and long retry limits respectively and CWmin and CWmax are minimum and maximum Contention Window sizes. All these simulations are performed for 2MHz bandwaidth and at 900MHz carrier frequency. Channel model and path loss model remain the same as described above.

T_{sym}	40 us
MAC header	14×8 bits
PHY header	6×T_{sym}
ACK	PHY header
RTS	20×8 bits + PHY header
CTS	PHY header
Basic data rate	650 Kbps (MCS 0)
SlotTime	52 us
SIFS	160 us
DIFS	SIFS + 2×SlotTime
m_{short}	7
m_{long}	4
CWmin	15
CWmax	1023

Figure 4.6 *Constant Parameters for IEEE 802.11ah*

4.3.5 Code Test

We tested the validity of code with the simple simulation of stations connecting to single AP, taken from [16] In this scenario, there were different number of STAs (from 1 to 100) with one AP. The scenario describes the range, throughput and colission rate while using Basic Access mechanism. Mcs 0 was used so the data rate, SINR and sensitivity was constant. and the transmitter power was 1mW. The physical placement of stations was from 0 to 342 m (0 to 342 on x and y axis both) randomly while AP was placed at 171,171 x,y coordinates in the playground. This was because the range for communication with 1mW transmit power is 171m so all the stations are considered to be in range of communication. The traffic interval used is 0.1 sec while the packet size is 256 Bytes. The diagrams for throughput in this thesis 4.7(b) and referenced Orod's theis 4.7(a) are shown below. These results show that the simulation code used in this thesis is correct and we can use implement other features on top of this code for this thesis.



(a) (b)

Figure 4.7 *Throughput for different number of nodes, (a) is from mentioned reference while (b) was the one resulted in simulations performed for this thesis*

4.4 Simulation scenarios

4.4.1 Assumptions / Parameters to simulations

Before discusing actual simulation scenarios, here are some assumptions and parameters used in the following simulations. Of course, there are some parameters which change with different simulations. For instance, number of nodes is different in different simulations depending upon the scenario we want to implement and what we want to test in that scenario, the distance between the STAs and AP is different as it is random within some defined boundary which means that there could be potentially hidden node situations. However some basic constants that we use throughout the simulation are as follows:

Traffic Parameters

Although IEEE 802.11ah is drafted to provide many traffic models but the one we are using is IoT based. The traffic model described for this protocol for IoT use case is that small packets of 256B in length are sent and the normal traffic interval between consecutive transmission can be 10 to 60 seconds. We are using 30 seconds as transmission interval in this thesis. The flow of traffic in these simulations is from Stations to Access Point. This is because when stations try to access the same

channel and multiple stations try to connect to AP so we simulate the situations when collision can happen and how the throughput and delay works out in such situation. For downwards communication when AP has to communicate to station, AP is the only entity in these simulations that hypothetically would be trying to communicate to stations so there are less chances of collision and also AP uses PCF to communicate to stations. So we are not simulating downwards traffic model in these simulations.

Physical Positions

Physical position of nodes (in case of 1 km transmitter power scenarios) is within 1 km diameter with AP at the center. However STAs are dispersed randomly by the simulator so such situations can arrive where some station nodes on the opposite side of AP start transmitting to AP without sensing each other's transmission. We are using RTS / CTS technique to cater for that situation. RTS / CTS reduces throughput for small sized networks but since we are simulating this network for 10s of nodes and IoT use case of IEEE 802.11ah protocol can accomodate hundreds of node, using RTS / CTS is better for overall throughput since it avoids collision caused by hidden nodes.

Sources of collision and Congestion Control

In the below mentioned simulations, there is only one AP before relays were implemented. After the implementation of relays, there were basically 2 APs and so the beacons received by STAs were also from 2 different APs. In that case, there is a chance of collision on the phy wireless layer and also on MAC layer. For MAC layer collision avoidance, we are using DCF along with CSMA which senses the medium before transmitting in order to avoid collision. RTS/CTS are also used to care for hidden node situations since the placement of nodes is random and there can be hidden node situations happening randomly in each run of simulation. Collision avoidence on PHY layer can still take place and one easy solution implemented in the simulations for this is to start APs and STAs at different times, this way they will send packets at different times on Phy layer and can avoid collision.

wireless collision in wireless medium, congestion can happen at any link when more

that one station is communicating. phy collisions vs MAC level collisions. Collision avoidance.

Association of STA to AP

The association of STA to AP is done by exchanging packets in a handshake process as mentioned in the draft of IEEE 802.11ah [39]. There are seperate authentication request, authentication response, association request and association response frames for that handshake mechanism. However, the basic idea for association of STA to AP that is implemented in these simulations is such that STAs receive beacons from different APs. The beacon signal received in STA with highest power amongst others is considered better than others and so the STA gets associated with the AP which sent this beacon.

Channel access

STAs use DCF for channel access while communicating to AP and the mechanism of DCF is described above. AP uses beacons to let STA know about itself. The channel model is outdoors . Channel access is implemented in MAC layer modelling in simulation .

Hierarchy of Network

Hierarchy of network is such that in the simulations without relays, stations connect to AP directly. This association is described above in above section. In relay-based simulations, stations are hard coded on the basis of their IP addresses and stations connect only to Relay AP and Relay Station associates to AP. This association in relay simulations ideologically bypasses the association procedure (since it is hard coded to associate to mentioned devices).

Sending and Receiving frames

The submodule which simulates higher layers (Session, Presentation and Applicatio) is called Management submodele. It has notification board from where we can see logs of what is happening in the simulation. Then we have WirelessSensorTrafficGenerator and WirelessSensorSink submodules which generate and receive data packets respectively. The parameters like delay and total number of successfully packets etc are tracked in WirelessSensorSink submodule.

Relaying of Packets in Relay

In this section we will explain how Relaying was implemented and how data is transfered from STA through Relay to final AP. Keeping in mind that Relay in itself is described here as Relay STA and Relay AP joined together as shown in 4.11. The functionality of Relay AP and Relay STA is also the same but just that the assoication to final AP is like this: STA devices send data to Relat AP, Relay AP relays/transfers the same data to Relay STA and this Relay STA then sends the data finally to destination AP. There were multiple ways of performing relaying in simulation: one way was to take the data packet received from STA in Relay AP and send that directly to Management layer of Relay STA using gates. Relay STA would then bypass its own data generation module and rather use this data received from gate (the original data from station transferred from Relay AP to Relay STA) and continue the functions of lower layers as normal eventually sending the data to destination AP. This technique of relaying reduced the work load of transferring only the data bits and creating a new packet using these data bits. Time overhead in relaying was also reduced using this method as the data packet is transfered directly and not re-created.

4.4.2 One Ap, One STA

This is a basic topology where we have one AP and one STA only. This scenario tests the range, delay and througput of the network through this topology. The Sinr, data rate and Path loss models are already described earlier in this chaper along with the mcs values and those remain the same throughout the thesis. The only limitation is for Transmitter power and according to FCC rules, it can go upto

a maximum of 1 Watt, in sub 1 GHz licence exempt band. [36]. This simulaiton scenario follows the use case of sensor networks and IoT, hence the given parameters are as proposed in the doc: [49] for this purpose.

Simulation Parameters for this scenario

AP nodes start sending beacons from 0 ms to 20 ms randomly while STA nodes start from 0 ms to 10 ms of simulation time.

The packet size for this use case is 256 Bytes, traffic interval is 10 to 60 secs (30 sec in these simulations) and Packet Error Rate for successful transmission should be less tahn 10 percent according to .11ah specification. In sensor networks for most of times only STA needs to send sensor data to AP so the direction of communication is from STA to AP and AP only sends control information to sensors and this trend follows all the below simulations. Sensors use CSMA/CA to avoid collisions and DCF for channel access, while in case of AP, it uses PCF for sending control packets to STAs. The physical location of STAs is such that station nodes are randomly spread between (0, 1076) as x and y coordinates while AP is located at (600,600). The x,y starts from 0,0 so the units for position can be considered as distance in m. The theoratical range supported by this use case is upto 1 km with minimum 100Kbps data rate, we will mention in the results how that theory measures up. This simulation was run for 3600 secs i.e. 1 Hr and the traffic interval is 30 sec so there were 120 total packets sent from station to AP, MCS0 was used so the basic datarate was 0.65Mbps. Calculated range is shown above, here is the simulated range i.e. 1000m between sensor and AP. The formula used for Throughput is : 4.5

$$\begin{aligned} Throughput &= BitsSent/UnitTime. \\ Throughput &= TotalNumOfBitsSent/TotalSimulationTime. \end{aligned} \tag{4.5}$$

Results

Throughput in this scenario comes out to be : 68.26666 (245760 bits sent within 3600 secs) with 0 collisions (only one station transmitting so the whole channel is available for this one station) and the average delay was 0.001652 secs i.e. 1.6 ms for 1km range. The data rate was 650000bps.

Calculation of Results

When the simulation finished, total number of bits successfully sent are calculated and divided by total simulation time to get overall Throughput. However, in this paticular scenario, since there was only one AP and one STA, this would be per node throughput as well. . The unit of throughput is bits / sec.
Range is the distance between sensor and AP which in this case was set manually in .ini file and is measured in meters or kilometers.
Delay is the time taken for the packet to be received by AP. The calculation formula would be then simulation time - packet transmission time. Average delay would be total delay (sum of delay in all the packets sent) / num of successfully recieved packets. As delay is quantity of time so the units are sec.

4.4.3 One AP serving up To Hundred STAs

In this section we will have a look at how AP responds to multiple stations uploading data, how many sensors sending data altogether ends up reducing the throughput and how long does it take to successfully transmit the data. The transmitter power used in this scenario is 1Watts (max transmitter power that can be used according to FCC rules [36].) and hence the range of communication (playground in this simulation) is about 1km. B.E.R, sensitivity and other parameters are still same as described above. The number of sensors in this scenario are 1, 10, 20, 30, 40, 50, 80 and 100 and all these stations are starting at arbitrary times between 0 and 20 secs with transmit interval as 30 sec. The physical position of all these station nodes is within 1 km (0,0 to 1km,1km) with AP in the center. The method of calculation of results is the same as described in earlier simulation. However, we also measure average per node throughput (average of throughput received per node, for any given number of nodes.) in addition to overall throughput of the network (total number of bits received during the whole simulation / total simulation time).

Results

The diagram 4.8 shows the average per node throughput of the network with mentioned number of stations sending data to AP. Notice that per node throughput value remains more or less constant at 0.68 Mbps with little variations upto 80 STAs.

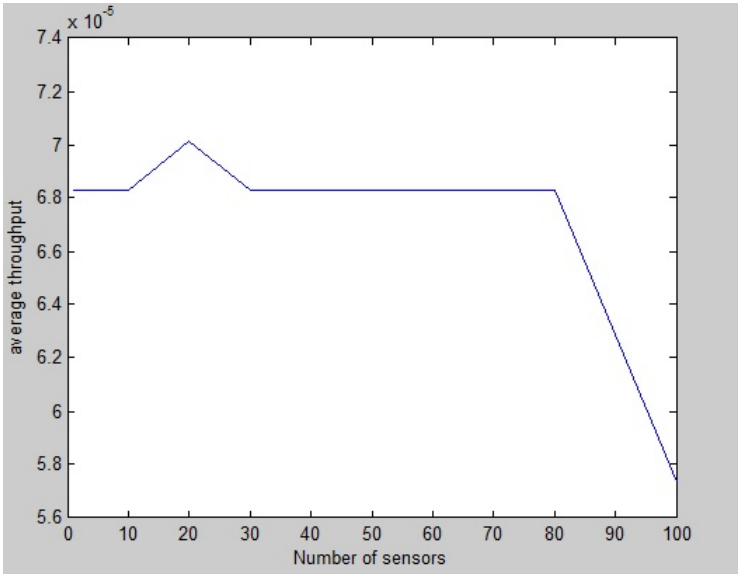


Figure 4.8 *Throughput (per node average, per packet) as calculated from station to AP communication, x-axis represents number of nodes while y-axis represents average per node per packet throughput in bits per seconds*

Figure 4.9 shows the overall network throughput with upto 100 nodes running for upto 1 hour as total simulation time with 30sec packet interval. The throughput keeps increasing as number of nodes increases up to 100, that is because the traffic interval for IoT use case is 1 packet of 256 Bytes every 30 secs, which means practically each node will be transmitting once a second. Since all the nodes are started at random intervals in this thesis and they are all transmitting randomly, there is enough room in the medium to support traffic from these devices and also there is RTS/CTS used for collision avoidence. So, up to 100 nodes with the mentioned parameters, there is a bearable amount of collision in channel access and sufficient data is still received correctly at destination. One point to notice is that the growth rate of throughput decreases after 80 nodes as more nodes are added in the network, this shows that after 80 nodes, under the mentioned parameters, the network starts to get a little congested, though still delivering good enough throughput.

Figure: 4.10 shows the end to end delay between nodes and AP and the units are mili-seconds. This delay is unidirectional time taken for sending data from station to AP. As we can clearly see in the figure obtained that the delay increases as the number of nodes are added in the network, this is because more nodes are now trying to connect to AP and RTS / CTS is also used, which also adds additional delay in the network but reduces probability of collision.

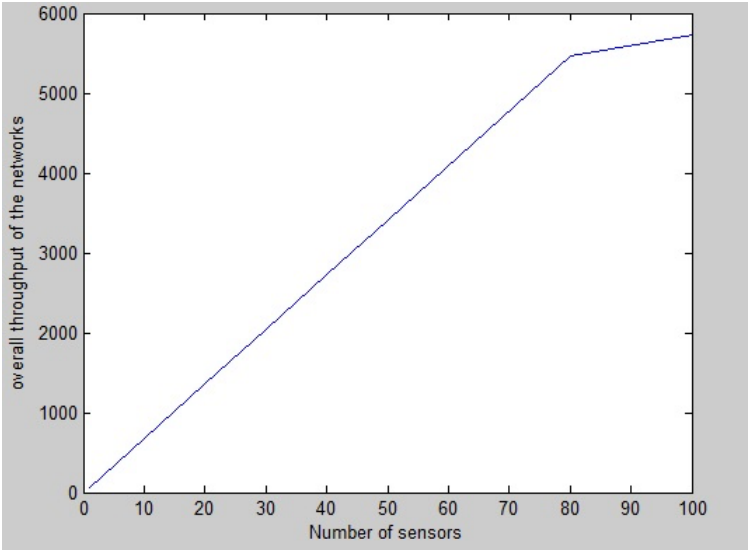


Figure 4.9 *Throughput (overall network) as calculated from final number of bits received in AP, x-axis shows number of nodes while y-axis represents overall network average throughput in bits per seconds*

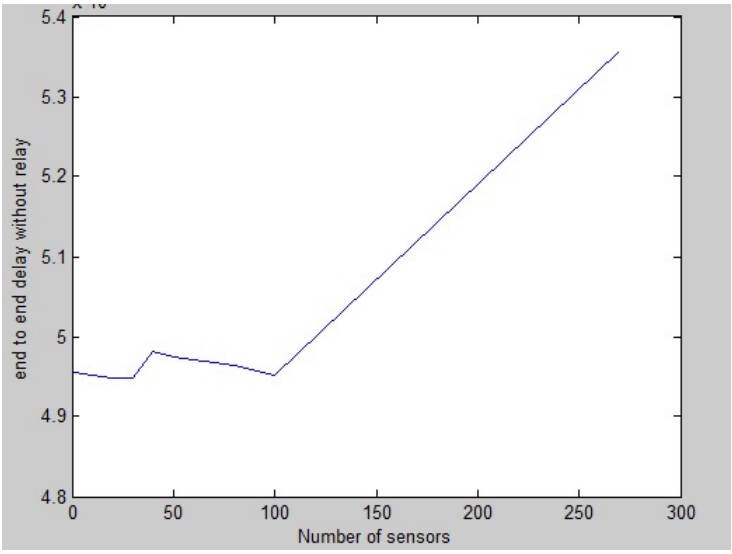


Figure 4.10 *Average overall end to end delay betwen stations and AP, number of nodes is on x-axis while delay is in mili-seconds on x-axis*

4.5 Relays

IEEE 802.11ah specification states that in order to increase range while still having better reception quality and throughput, we can introduce relays in the network. Relays keep the signal strength high enough while still communicating at longer ranges. Relays are simply data forwarding devices, which receive data from stations and forward that to the AP which they are connected to. [39].

4.5.1 Functionality of Relays

In IEEE 802.11ah draft 8.0 [39], the way these relays are configured and work is that a relay is made of relay station and relay AP working together, so basically wireless stations connects to relay AP first, relay AP receives packets from stations, transfers them to relay station and this relay station then transfers those packets to the AP. The funtion of relay can be triggered on and off in the control messages. But in this simulations, relays are working manually, just to check the performance of the network using relays. The figure 4.11 shows the ned file with relays explaining the data flow and functionality of relays. As already mentioned in the simulator settings section, relay works as a combination of station and AP, only difference is that they are called Relay Station and Relay AP since they are part of Relay and also the data flowing through Relay is not generated in Relay , but is the original data which was sent from source station. In this simulation, time taken for data transfer from Relay AP to Relay Station was checked and confirmed to be 0ms, which should be the case meaning that relay device itself is not adding much of delay towards the overall data transfer, ofcourse the radio in Relay devices would add some delay because of sensing mechanisms and DCF. Important thing here is that collissions during the delivery of packets doesn't temper with the delay or throughput calculations since delay is calulated by taking the difference of current simulation time and message creation time. So, whenever the collision happened in the channel, and the node had to wait and resend, when it found the channel to be free, message creation time would still be same, so the results should be correct. Also delay is now (delay from sta to relay + delay from relay to AP) and this delay includes the wait and retransmission time in case of collision.

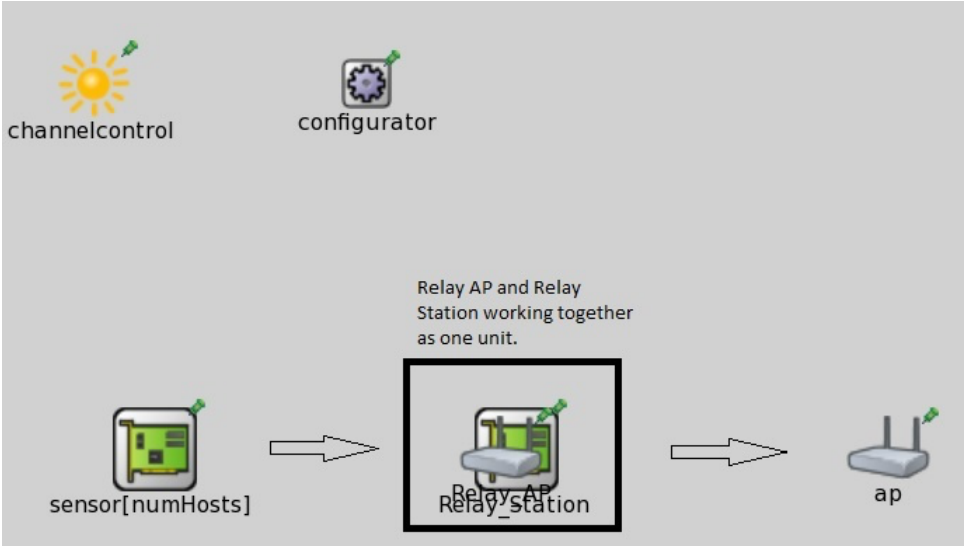


Figure 4.11 *NED file representing data flow from station through relay to AP.*

4.5.2 One Relay, One AP, Multiple STAs

Again, we are using 1W transmitter power to check the maximum range which can be achieved using relays, the total playground is about 2 km now (2000, 750)m, and the rest of simulation parameters e.g. traffic parameters, radio parameters etc are same as above scenario without relays. MCS 0 was used in this simulation as well. We placed multiple sensors which were first connecting / associating to relay and relay was then transfering the packets to AP.

physical placement of devices

The physical placement of Stations was such that all the stations were radomly gathered around within x-axis ranging from 0 to 1 km while y axis ranging from 0 to 700m. The location of AP was (1810, 375)m, while the location of relay was (740, 375)m, so the distnace between relay and AP was 1070 meters. STAtions / sensors were gathered randomly around relay.

Calculation of Results

Since in these simulations, throughput calculations are overall for the whole network, we calculated throughput using relays in the same way. As the total simulation time

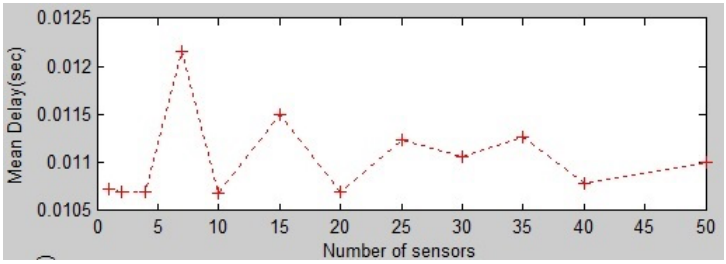


Figure 4.12 *Delay with one relay and one AP in the network. x-axis shows the number of nodes while y-axis represents the delay per node per packet delay in seconds.*

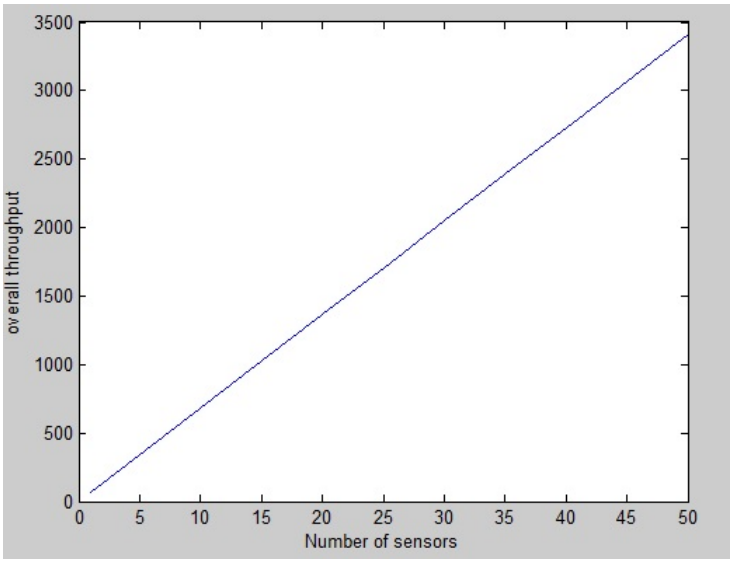


Figure 4.13 *Overall Network throughput with one relay and one AP in the network. x-axis shows number of nodes in the network while y-axis shows throughput values in bits per second.*

and number of packets sent during this simulation time are same, there is not much of difference in overall throughput of the network up to 100 nodes.

Figure 4.13 shows the overall throughput of 50 nodes in the network with relay. Figure 4.14 shows the average per node network throughput of the relayed network while 4.12 shows the mean (per node) delay against number of nodes for this simulation. Note that this delay is mean so its an average of total time taken for successful number of bits received eventually by AP (the ones that got transmitted in the first try and also the ones that collided and had to be retransmitted).

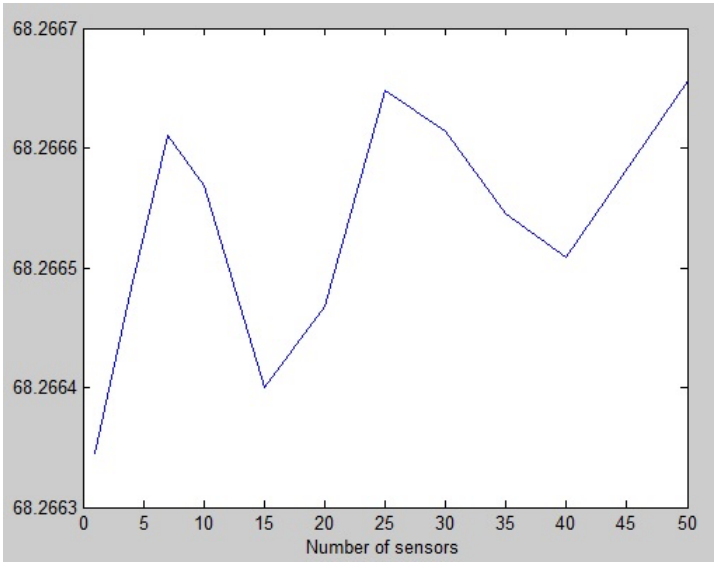


Figure 4.14 *Average per node per packet throughput with one relay and one AP in the network. x-axis shows number of nodes while y-axis shows throughput values in bits per second*

4.6 Difference after relaying

In this section we will demonstrate the difference between the simulation results obtained before relaying and after relaying was implemented. Figure 4.15 shows that the delay without relaying is quite less as compared to delay of the scenario with relay implemented in it. The units for both graphs are seconds. As it is clear the units on y-axis for the end to end delay without delay is 10 power -3 meaning these y axis values correspond to mili-seconds while delay values for the graph after implementation of relays shows values in seconds. For instance, for 40 nodes in the network without relay, the average delay for average packet per node in the network is roughly 4.98 mili-seconds whereas average delay for average packet per node in the network where data was flowing through relay was 0.0108 seconds i.e. 10.8 mili-seconds. With this extra delay, by taking a look at the above scenarios and results, we can safely say that Relaying almost doubles the delay and range while overall throughput of network remains almost the same until the number of nodes get too much and number of collisions in the network gets unacceptable.

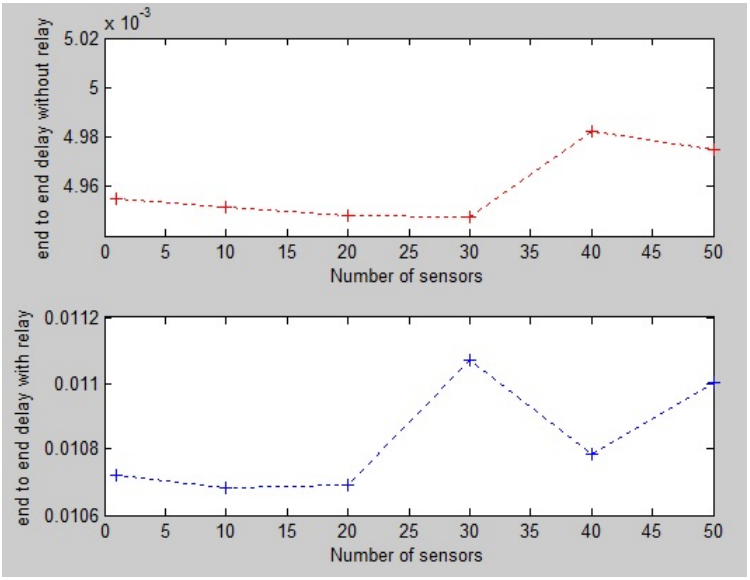


Figure 4.15 *Difference between delay values for nultiple nodes without and with relay*

5. CONCLUSION / ANALYSIS OF IEEE 802.11S AND IEEE 802.11AH

The main idea of this thesis was to study and analyze the networking protocols and their performance in IEEE 802.11s mesh networks and IEEE 802.11ah IOT use case. The results of analysis are shown in their respective chapters. However, for the sake of conclusion, we will mention the results here too. The language of programming for this thesis was C++ and the simulator used was Omnet++. This chapter is organized such that in the next section, we will mention the performance of both protocols based on the simulations we performed, the pros and cons and then the comparison of these technologies. Then comes the co-existance of these technologies and some future proposals. The data flow in both technologies is unidirectional (uplink in 802.11ah while downlink in 802.11s). IEEE 802.11s implementation uses EDCA while IEEE 802.11ah implementation uses DCF. The metric of performance is overall network throughput and mean overall delay (average taken from all nodes).

5.1 IEEE 802.11ah performance

In this case we evaluate the performance of IEEE 802.11ah before and after relay implementation. Even though 1W transmit power is not realistic, it still gives us feasible comparison for relay implementation. Since in this thesis, we are calculating overall throughput which depends on the traffic interval, bit error rate, simulation time ets and those parameters are same in both scenarios, so, the average per node throughput values for both scenarios is 68.266 bits/sec. The main difference can be seen in relaying and range of communication, The ranges almost doubles with the use of relay since the distance from far most station to relay can be same as from relay to AP. Figure 4.15 shows that there is much more delay in transferring the same amount of data at the same traffic interval after the implementation of relays because data had one extra hop to travel beofre it reaches the final destination i.e. AP. Note here that the destination is set manually in this simulation and no routing

protocol is used.

The conclusion deducted from this simulation is that the range of communication can be doubled in IEEE 802.11ah at the cost of delay and throughput. Therefore, for use cases like temperature, pressure, humidity sensing etc, the delay or throughput can be bearable as long as the transmisison range covers all the far located sensors with acceptable Bit Error Rate. Also in latest draft of IEEE 802.11ah [39], multihop relays are introduced which means that more than one relay can be used in the same network. SubFields in control packets indicate whether to turn relays on or off and also AP can indicate how many number of relays can be allowed based on the link and traffic situation .

5.2 IEEE 802.11s performance

IEEE 802.11s mesh uses a sophisticated suite of networking protocols for its operation. It has HWMP as mandatory networking protocol which has both proactive and on-demand type of networking available. For proactive networking, 802.11s creates a tree like structure while setting up the network to create routes for all possible destinations. It does so by suing OLSR as routing protocol and airtime metric. Whenever any link fails, RERR messages are sent down the tree from the point where the tree link was broken and alternate routes are calulated from the Hello messages information. The simulation performed for this thesis had the whole MAP and MPs setup in it before the request reaches MPP so the number of relays in the network is more than number of relays in IEEE 802.11ah. But this is the functionality of mesh networks and we simulated this network in its natural way of working. Conclusively, figure 3.7 shows that overall throughput decreases as we add nodes to the network. This is because intermediate nodes are not only carrying their own requested data but also acting as relays for other nodes so the overall network performance decreases. It surely also depends on the traffic model used. Traffic model in this 802.11s simulation is quite different from normal IoT use case so these two technologies cannot directly be compared but the network performance can be judged in their own natural capacity.

5.3 Comparison of IEEE 802.11s and IEEE 802.11ah networks

IEEE 802.11s and 802.11ah are two different technologies working on different radios and are designed for different purposes. Although both are used for wireless sensor networks but the specific use cases are more peculiar e.g. mesh network is used for more crowded and dense areas since the same traffic can get multiple paths and still reach the station. Link failures don't affect too much and user can still get connectivity. So one best possible scenario for mesh network is e.g. public WiFi access in city center or other public areas .
On the other hand 802.11ah is designed for IoT use cases where sensing devices need to send data and the network traffic is not fully loaded all the time. So range and battery consumption is the focus point in this technology. That is why IEEE 802.11ah is best for this purpose as we saw in the simulation that reaching far away nodes of upto a km is possible in 802.11ah. Sure the datarate used in this case would be less but for sensing devices, its perfectly fine. Also devices go to sleep mode in IoT use case is a lot more than 802.11ah. Even the AP in 802.11ah can go to sleep mode to save energy while the higher end relaying devices (MPPs) in mesh networks connect this mesh network to other networks so they cannot go to sleep mode.
The network traffic in IEEE 802.11ah IOT use case is less as compared to IEEE 802.11s. The range requirement of IEEE 802.11ah is quite high while 802.11s can only reach a little over 100m (140 theoratically). The routing overhead would be too much if any routing protocol would be implemented in IEEE 802.11ah and so IEEE already introduced multihop routing in the specification [39] to mitigate this issue. Also this improves the overall efficiency since individual links from nodes to Relay don't get overloaded. IEEE 802.11ah has a more clear and concise way of data transfer which helps these computing devices of these days transfer data efficiently which not adding too much overhead to the network. More detailed concerns about real life implementations and challanges of IoT are discussed in [33]

5.4 Co-existence and future Enhancements

Since there is a specific node in IEEE 802.11s called MPP whose task is to connect this wireless mesh network to other networks, IEEE 802.11ah can connect from ethernet or WiFi to this node and both these technologies can co-exist.

6. SIMULATOR

We modelled the behaviour of a real life network in a network simulator for this study. There are many network simulators available in market. Some are proprietary liscenced (e.g. OPnet and NetSim) and users have to pay to use those while others are open source and users don't have to pay to use them e.g. NS and OMNET++. Our choice of simulator was OMNET++ because its open sourced, has huge support community and frameworks like Inet and Inetmanet etc and also our department already has some nice implementations of protocols in OMNET++. Omnet++ has quite nice GUI visuals embedded so users can have a real time look at network and packets flowing within the network but for people who like to work with command line, Omnet++ can be used via command line with no visuals as well.

6.1 Omnet++

Omnet++ is an event based, discrete event, open source network simulator with many inbuilt communication frameworks like queuing networks, digital logics networks etc. It is available for Windows and Unix / Linux like Operating Systems and one good thing about it is that it is installed in a folder locally in Unix based OSs, which means one doesn't have to install it globally for the whole system rather one can install many instances of it in different folders. In Windows based systems, there are .exe files to install it while in Unix like systems, it works like many other native software programs of Unix i.e. ./make and ./configure. MACintosh systems being built on a Unix Like system in its base technology, also supports Omnet++. There are some pre-defined examples in examples filder to get started with the How To Use process. [50]

6.1.1 Main Components

Omnet++ operates with some main components, mainly Modules and files for that module. There are simple modules that can be combined to make complex module to make networks , topologies and infrastructures. These modules show graphically what any component is and then have the code file along with it to tell the compiler how this component works. There are 3 types of files to run these complex modules. Ini file is initial file to set the parameters for the simulation. NED file is linked with GUI components to to programatically explain what that component would take in as parameter, how many gates/connections would it have and how many subcomponents it would have. Then there are C++ files for the actual task that the component performs. For any network, simulation starts with .ini file. There are very nice tutorials on how to get going with all these basics e.g. Tic Toc tutorial [51] explains how to make a simple scenario where 2 nodes send data back and forth to each other and then take statistics.

6.1.2 Designing a network in Omnetpp

Designing a network from scratch is easy in Omnet++ . User starts with the simplest possible component, define and design it correctly and then join together more components to make a complex component. Many complex components can then be used to make a network. Each component has ned and c++ file which describes the parameters and working of that component respectively. [52]

6.1.3 Coding in Omnetpp

Network infrastructures are coded in NEtwork Description language (NED) in omnet++. The structure of code is quite easy and explained in [53] in detail. The logic coding of simulations in omnet++ is done in C++. C++ is quite old programming language (developed in 1983) which gets modified time to time. Because of being around for such a long time (about 33 years so far), there are enormous amount of code and support available on the internet to learn C++. The most authentic information about C++ can be found from their website: [54]

6.1.4 Getting statistics in Omnetpp

Omnet++ has a procedure for collecting statistics during or after a simulation is finished. There are WATCH parameters which track the value of parameters during the simulation and user can also RECORD SCALAR in the finish function of the program to list the values after the simulation is finished. There is also an option for elog file creation which graphically shows all the nodes and messages going in between them. This elog file is a nice way of troubleshooting if something goes wrong. [55]

REFERENCES

[1] "History of ieee," August 2016. Available at: https://www.ieee.org/about/ieee_history.html.

[2] L. S. Y. Z. X. P. C. B. W. Guido R Hiertz, Dee Denteneer, "The ieee 802.11 universe," Jan 2010.

[3] "Ieee 802.11: Wireless lans." Available at: http://standards.ieee.org/about/get/802/802.11.html.

[4] "Internetworking basics," *Cisco Press*, 1989 - 1998. Available at: http://www.cisco.com/cpress/cc/td/cpress/fund/ith/ith01gb.htm#xtocid166844.

[5] N. Instruments, "What is a wireless sensor network ?," May 2016. Available: http://www.ni.com/white-paper/7142/en/.

[6] "Ieee 802.11 architecture," Feb, 2013. Available at: http://www.tutorial-reports.com/wireless/wlanwifi/wifi_architecture.php.

[7] S. Ranvier, "Physical layer methods in wireless communication system: Path loss models," *HELSINKI UNIVERSITY OF TECHNOLOGY, SMARAD Centre of Excellence*, Nov, 2004. Available at: http://www.comlab.hut.fi/opetus/333/2004_2005_slides/Path_loss_models.

[8] P. M. Torlak, "Telecom. switching and transmission: Path loss," *UT Dallas*. Available at: https://www.utdallas.edu/~torlak/courses/ee4367/lectures/lectureradio.pdf.

[9] "Receiver sensitivity / noise." Available at: http://www.phys.hawaii.edu/~anita/new/papers/militaryHandbook/rcvr_sen.pdf.

[10] M. M. da Silva, "Cable and wireless networks: Theory and practice," p. 700, Jan. 2016.

[11] M. Loy, "Understanding and enhancing sensitivity in receivers for wireless applications," May. 1999. Available at: http://www.ti.com/lit/an/swra030/swra030.pdf.

[12] J. Tourrilhes, "ch5, the mac level (link layer)," Available at: http://www.labs.hpe.com/personal/Jean_Tourrilhes/Linux/Linux.Wireless.mac.html.

[13] F. S. B. Y. Costas Busch, Malik Magdon-Ismail, "Contention free mac protocols for wireless sensor networks," Available at: `https://www.cs.rpi.edu/research/pdf/04-12.pdf`.

[14] S. Kurkovsky, "Computer networks: Multiple access protocols, link layer addressing." Available at: `http://www.cs.ccsu.edu/~stan/classes/cs490/slides/networks4-ch5-2.pdf`.

[15] A. C. Snoeren, "Carrier sense multiple access," 2013. Available at: `https://cseweb.ucsd.edu/classes/fa13/cse123-a/lectures/123-fa13-l8.pdf`.

[16] O. Raeesi, "System-level performance analysis and optimization of ieee 802.11ah – the new sub-1 ghz wi-fi." IEEE, Oct, 2013. Available: `http://dspace.cc.tut.fi/dpub/handle/123456789/21780`.

[17] "Wifi 802.11 wireless lan,." Available at: `http://www.cs.montana.edu/~halla/csci466/lectures/lec11-2.8-wifi.html`.

[18] R. Jain, "Wireless local area networks (wlans) part 1," *Washington University in Saint Louis*, . 2010.

[19] J. B. C. Saikat Ray and D. Starobinski, "Rts/cts induced congestion in ad-hoc wireless lans," Available at: `http://people.bu.edu/staro/wcnc-ray.pdf`.

[20] K. J. K. J. C. Z. W. Steven Conner, Jan Kruys, "Overview of the ammendment for wireless local area mesh networking," *IEEE 802.11s Tutorial*, Nov. 2006.

[21] CalsoftLabs, "Wireless 802.11s mesh networks, a techno coommercial,"

[22] J. Monza, "Wireless networking basics for business." Available at: `http://www.securedgenetworks.com/blog/3-Key-Benefits-of-Wireless-Mesh-Networks`.

[23] P. S. S. Sampio and F. Vasques, "A review of scalability and topology stability issues in ieee 802.11s wireless mesh network deployments," vol. 4, Dec. 2014.

[24] C. Press, "Routing protocol selection guide - igrp, eigrp, ospf, is-is, bgp,"

[25] P. J. Network Working Group: T Clausen, "Optimized link state routing protocol," oct 2003. Available at: `https://tools.ietf.org/html/rfc3626#page-9`.

[26] S. Network Working Group: C Perkins, E Belding-Royer, "Ad-hoc on-demand distance vector aodv routing," July 2003. Available at: `https://tools.ietf.org/html/rfc3561`.

[27] D. C. M. S. L. H. M. K. C. Miguel Elias M. Campista, Pedro Miguel Esposito, "Routing metrics and protocols for wireless mesh networks," p. 30.

[28] F. Y. L. Thomas Aure, "An optimized path-selection using airtime metric in olsr networks: implementation and testing," *2008 IEEE Symposium for Wireless Communication Systems*, pp. 9–11, Oct. 2008.

[29] I. C. Society, "Ieee standard for information technology telecommunications and information exchange between systems, local and metropolitan area networks, specific requirements. wireless lan medium acess control mac and physical layer phy specifications, ammendment 10: Mesh networks," p. 372, September 2011.

[30] A. A. Q. Behrang Barekatain, Mohd Aizaini Maarof and A. T. Cabrera, "Greenie: A novel hybrid routing protocol for efficient video streaming over wireless mesh networks.," *Journal on Wireless Communications and Networking 2013*, May 2013.

[31] A. A. V. Alfonso Ariza Quintana, "Inetmanet 2.0 framework," *Github code base*, vol. 1.

[32] "Internet of things, overview," Available: `http://www.cisco.com/c/en/us/solutions/internet-of-things/overview.html?`

[33] L. C. Karen Rose, Scott Eldridge, "The internet of things: An overview," Oct, 2015. Available: `http://www.internetsociety.org/sites/default/files/ISOC-IoT-Overview-20151022.pdf`.

[34] A. A. Yongho Seok, Zander Lei, "Status of project ieee 802.11ah." IEEE, Oct, 2016. Available: `http://www.ieee802.org/11/Reports/tgah_update.htm`.

[35] I. Poole, "Ieee 802.11ah - sub ghz wi-fi," Available: `http://www.radio-electronics.com/info/wireless/wi-fi/ieee-802-11ah-sub-ghz-wifi.php`.

[36] M. Cheong, "Fcc rules for unlicensed wireless equipment operating in the ism bands," Available: `http://www.afar.net/tutorials/fcc-rules`.

[37] V. E. Ron Porat, "Outdoor path loss models for 802.11ah," Feb 2011. Available: https://mentor.ieee.org/802.11/dcn/11/11-11-0272-00-00ah-outdoor-path-loss-models-for-802-11ah.ppt.

[38] Atmel, "Range calculation for 300mhz to 1000mhz communication systems," Available: http://www.atmel.com/Images/Atmel-9144-Range-Calculation_Application-Note.pdf.

[39] IEEE, "Draft standard for information technology, telecommunications and information exchange between systems, local and metropolitan area networks, specific requirements. part 11: Wireless lan medium access control and physical layer specifications," *IEEE 802.11ah Draft 8.0*, April. 2016.

[40] Q. Z. X. S. Haitao Wu, Xin Wang, "Ieee 802.11e enhanced distributed channel access (edca) throughput analysis," 2006. Available: http://ieeexplore.ieee.org/xpl/login.jsp?tp=&arnumber=4024121&url=http%3A%2F%2Fieeexplore.ieee.org%2Fstamp%2Fstamp.jsp%3Farnumber%3D4024121.

[41] D. Ramana, "Rate adaptation in 802.11 networks," Available: http://home.iitj.ac.in/~ramana/802-11-rate.

[42] S. Herbert, "Advanced wireless local area networks in the unlicensed sub-1 ghz ism-bands." TU Delft, Oct, 2014. Available: http://www.es.ewi.tudelft.nl/phd-theses/2014-Aust.pdf.

[43] D. H. Stefan Aust, Jae-Hyung Song, "Proposed ieee 802.11ah use cases," Jan, 2011. Available: https://mentor.ieee.org/802.11/dcn/11/11-11-0017-00-00ah-proposed-ieee-802-11ah-use-cases.pdf.

[44] "Ieee iot scenario and use cases: Social sensors," Feb, 2013. Available at: http://iot.ieee.org/images/files/pdf/scenarios/IEEE_IoT_Service_UseCases_Social_Sensors_clean.pdf.

[45] R. V. P. . I. G. M. M. N. Stefan Aust, "Ieee 802.11ah: Advantages in standards and further challenges for sub 1 ghz wi-fi," june, 2012. Available: http://ieeexplore.ieee.org/xpl/login.jsp?tp=&arnumber=6364903&url=http%3A%2F%2Fieeexplore.ieee.org%2Fstamp%2Fstamp.jsp%3Ftp%3D%26arnumber%3D6364903.

[46] T. I. Stefan Aust, "Sub 1ghz wireless lan deployment scenarios and design implications in rural areas," 2011. Available at: http://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=6162336&tag=1.

[47] R. de Vegt, "Ieee 802.11ah benefits and use cases," July, 2015. Available: http://www.comsocscv.org/docs/IEEE%20ComSoc_11ah_Opportunity_V6_0715.pdf.

[48] R. V. P. Stefan Aust, "Ieee 802.11ah: Advantages in standards and further challenges for sub 1 ghz wifi," Available: https://www.semanticscholar.org/paper/IEEE-802-11ah-Advantages-in-standards-and-further-Aust-Prasad/db220b218d9451374fa8805c62f8b94f32110f7c/pdf.

[49] M. Cheong, "Tgah functional requirements and evaluation methodology rev. 0134," Sept, 2011.

[50] B. Ricks, "Omnet++ - tutorial 1," Available at: http://mews.sv.cmu.edu/teaching/14814/s14/files/14814s14_t1.pdf.

[51] Omnet++, "Tictoc tutorial for omnet++," Available: https://omnetpp.org/doc/omnetpp/tictoc-tutorial/.

[52] B. Y. University, "Omnet++ tutorial." Internet Lab Research: Brigham Young University. Available: http://ilab.cs.byu.edu/wiki/Omnet%2B%2B_Tutorial.

[53] "Omnet++ discrete event simulator." IEEE, Nov 1999. Available: http://www.ewh.ieee.org/soc/es/Nov1999/18/ned.htm.

[54] bjarne stroustrup, "C++," 1983. Available: http://www.cplusplus.com/doc/tutorial/.

[55] Omnet++, "Omnet++ documentation and tutorials." Available: https://omnetpp.org/documentation.

APPENDIX A. IEEE802.11AH CODE OF SIMULATION

The code for IEEE 802.11ah radio model is pasted here to see how physical layer is modelled in Omnetpp.

```
bool Ieee80211ahRadioModel::isReceivedCorrectly(AirFrame *airframe,
  const SnrList& receivedList)
{
    // calculate snirMin
    double snirMin = receivedList.begin()->snr;
    for (SnrList::const_iterator iter = receivedList.begin();
      iter != receivedList.end(); iter++)
        if (iter->snr < snirMin)
            snirMin = iter->snr;
    cPacket *frame = airframe->getEncapsulatedPacket();
    EV << "packet (" << frame->getClassName() << ")" << frame->getName()
    << " (" << frame->info() << ") snrMin=" << 10*log10(snirMin) << endl;
    RecvQuality *recvq = new RecvQuality;
    recvq->setSinr(snirMin);
    airframe->setControlInfo(recvq);
    if (snirMin < snirThreshold)
    {
        // if snir is too low for the packet to be recognized
        EV << "COLLISION! Packet got lost\n";
        return false;
    }
    else if (isPacketOK(snirMin, airframe->getEncapsulatedPacket()->
      getBitLength(), airframe->getBitrate()))
    {
        EV << "packet was received correctly, it is now handed to
        upper layer...\n";
        return true;
    }
    else
    {
        EV << "Packet has BIT ERRORS! It is lost!\n";
        return false;
    }
}
bool Ieee80211ahRadioModel::isPacketOK(double snirMin,
  int lengthMPDU, double bitrate)
```

```
{
    double berHeader, berMPDU;
    double headerNoError, MpduNoError;
    berHeader = ber_bpsk(snirMin, bandWidth, basicBitrate, channelModel);
    berHeader = Pb(1, berHeader);
    headerNoError = pow(1.0 - berHeader, PHY_HEADER_LENGTH);
    if(snrThresholdOverBER) {
        if ((unsigned)lengthMPDU > LENGTH_RTS) {
            double requiredSnir;
            if (bitrate == 0.650e6)
                requiredSnir = 11.41;
            else if (bitrate == 1.300e6)
                requiredSnir = 14.45;
            else if (bitrate == 1.950e6)
                requiredSnir = 17.12;
            else if (bitrate == 2.600e6)
                requiredSnir = 20.39;
            else if (bitrate == 3.900e6)
                requiredSnir = 23.76;
            else if (bitrate == 5.200e6)
                requiredSnir = 28.18;
            else if (bitrate == 5.850e6)
                requiredSnir = 29.76;
            else if (bitrate == 6.500e6)
                requiredSnir = 30.89;
            else if (bitrate == 7.800e6)
                requiredSnir = 36.09;
            EV << "snirMin: " << 10*log10(snirMin) << "! requiredSnir: "
            << requiredSnir << "! lengthMPDU: " << lengthMPDU <<
            "! bitrate: " << bitrate << endl;
            if (10*log10(snirMin) <= requiredSnir)
            {
                MpduNoError = 0; // error
            }
            else
            {
                MpduNoError = 1; // no error
            }
        }
        // rest of piece of code is not shown here.
    }
}
```